

**BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS**

10 december 2025

WETSONTWERP
houdende diverse bepalingen**Verslag van de tweede lezing**
namens de commissie
voor Financiën en Begroting
uitgebracht door
de heer **Vincent Van Quickenborne**

*Zie:***Doc 56 0963/ (2024/2025):**

- 001: Wetsontwerp.
- 002: Advies van de Gegevensbeschermingsautoriteit.
- 003 tot 011: Amendementen.
- 012: Verslag (Justitie).
- 013: Verslag van de eerste lezing (Sociale Zaken).
- 014: Artikelen aangenomen in eerste lezing (Sociale Zaken).
- 015: Zaak zonder verslag (Mobiliteit) (art. 78.7 Rgt.)
- 016: Amendementen.
- 017: Verslag van de eerste lezing (Sociale Zaken).
- 018: Artikelen aangenomen in eerste lezing (Sociale Zaken).
- 019: Verslag van de eerste lezing (Financiën).
- 020: Artikelen aangenomen in eerste lezing (Financiën).
- 021 en 022: Amendementen.
- 023: Verslag van de tweede lezing (Sociale Zaken).
- 024: Verslag van de tweede lezing (Sociale Zaken).
- 025: Verslag (Gezondheid en Gelijke Kansen).
- 026 tot 028: Amendementen.

Zie ook:

- 030: Tekst aangenomen door de commissies.

**CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE**

10 décembre 2025

PROJET DE LOI
portant des dispositions diverses**Rapport de la deuxième lecture**
fait au nom de la commission
des Finances et du Budget
par
M. Vincent Van Quickenborne

*Voir:***Doc 56 0963/ (2024/2025):**

- 001: Projet de loi.
- 002: Avis de l'Autorité de protection des données.
- 003 à 011: Amendements.
- 012: Rapport (Justice).
- 013: Rapport de la première lecture (Affaires sociales).
- 014: Articles adoptés en première lecture (Affaires sociales).
- 015: Affaire sans rapport (Mobilité) (Art. 78.7 Rgt.)
- 016: Amendements.
- 017: Rapport de la première lecture (Affaires sociales).
- 018: Articles adoptés en première lecture (Affaires sociales).
- 019: Rapport de la première lecture (Finances).
- 020: Articles adoptés en première lecture (Finances).
- 021 et 022: Amendements.
- 023: Rapport de la deuxième lecture (Affaires sociales).
- 024: Rapport de la deuxième lecture (Affaires sociales).
- 025: Rapport (Santé et de l'Égalité des chances).
- 026 à 028: Amendements.

Voir aussi:

- 030: Texte adopté par les commissions.

02614

**Samenstelling van de commissie op de datum van indiening van het verslag/
Composition de la commission à la date de dépôt du rapport**

Voorzitter/Président: Steven Vandeput

A. — Vaste leden / Titulaires:

N-VA	Wim Van der Donckt, Steven Vandeput, Charlotte Verkeyn
VB	Lode Vereeck, Wouter Vermeersch
MR	Mathieu Michel, Benoît Piedboeuf
PS	Hugues Bayet, Frédéric Daerden
PVDA-PTB	Kemal Bilmez, Sofie Merckx
Les Engagés	Xavier Dubois, Stéphane Lasseaux
Vooruit	Niels Tas
cd&v	Koen Van den Heuvel
Ecolo-Groen	Dieter Vanbesien
Open Vld	Alexia Bertrand

B. — Plaatsvervangers / Suppléants:

Peter Buysrogge, Eva Demesmaeker, Kathleen Depoorter, Michael Freilich
Dieter Keuten, Kurt Moons, Reccino Van Lommel
Pierre Jadoul, Florence Reuter, Vincent Scourneau
Khalil Aouasti, Pierre-Yves Dermagne, Christophe Lacroix
Raoul Hedebouw, Peter Mertens, Annik Van den Bosch
Luc Frank, Serge Hilgsmann, Ismaël Nuino
Jan Bertels, Jeroen Soete
Steven Matheï, Nathalie Muylle
Meyrem Almaci, Sarah Schlitz
Steven Coenegrachts, Vincent Van Quickenborne

N-VA	: Nieuw-Vlaamse Alliantie
VB	: Vlaams Belang
MR	: Mouvement Réformateur
PS	: Parti Socialiste
PVDA-PTB	: Partij van de Arbeid van België – Parti du Travail de Belgique
Les Engagés	: Les Engagés
Vooruit	: Vooruit
cd&v	: Christen-Democratisch en Vlaams
Ecolo-Groen	: Ecologistes Confédérés pour l'organisation de luttes originales – Groen
Open Vld	: Open Vlaamse liberalen en democraten
DéFI	: Démocrate Fédéraliste Indépendant
ONAFH/INDÉP	: Onafhankelijk-Indépendant

Afkorting bij de nummering van de publicaties:		Abréviations dans la numérotation des publications:	
DOC 56 0000/000	Parlementair document van de 56 ^e zittingsperiode + basisnummer en volgnummer	DOC 56 0000/000	Document de la 56 ^e législature, suivi du numéro de base et numéro de suivi
QRVA	Schriftelijke Vragen en Antwoorden	QRVA	Questions et Réponses écrites
CRIV	Voorlopige versie van het Integraal Verslag	CRIV	Version provisoire du Compte Rendu Intégral
CRABV	Beknopt Verslag	CRABV	Compte Rendu Analytique
CRIV	Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toezpraken (met de bijlagen)	CRIV	Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)
PLEN	Plenum	PLEN	Séance plénière
COM	Commissievergadering	COM	Réunion de commission
MOT	Moties tot besluit van interpellaties (beigekleurig papier)	MOT	Motions déposées en conclusion d'interpellations (papier beige)

Inhoud	Blz.	Sommaire	Pages
I. Inleidende uiteenzetting	4	I. Exposé introductif.....	4
II. Algemene bespreking.....	5	II. Discussion générale.....	5
A. Vragen en opmerkingen van de leden.....	5	A. Questions et observations des membres.....	5
1. Vergadering van 21 oktober 2025.....	5	1. Réunion du 21 octobre 2025.....	5
2. Vergadering van 4 november 2025.....	14	2. Réunion du 4 novembre 2025.....	14
3. Vergadering van 5 november 2025.....	34	3. Réunion du 5 novembre 2025.....	34
4. Vergadering van 12 november 2025.....	52	4. Réunion du 12 novembre 2025.....	52
5. Vergadering van 18 november 2025.....	155	5. Réunion du 18 novembre 2025.....	155
B. Antwoorden van de minister	328	B. Réponses du ministre	328
C. Replieken van de leden	354	C. Répliques des membres	354
D. Bijkomende antwoorden van de minister	392	D. Réponses complémentaires du ministre	392
E. Bijkomende replieken van de leden en de minister	395	E. Répliques complémentaires des membres et du ministre	395
III. Artikelsgewijze bespreking.....	399	III. Discussion des articles.....	399
IV. Stemmingen	429	IV. Votes.....	429
Bijlage: wetgevingstechnische nota	444	Annexe: note de légistique	453

DAMES EN HEREN,

Uw commissie heeft dit wetsontwerp besproken tijdens haar vergaderingen van 21 oktober, 4 november, 5 november, 12 november, 18 november en 25 november 2025.

I. — INLEIDENDE UITEENZETTING

De heer Jan Jambon, vice-eersteminister en minister van Financiën en Pensioenen, belast met de Nationale Loterij en de Federale Culturele Instellingen, verstrekt de volgende verduidelijkingen naar aanleiding van de wetgevingstechnische nota van de dienst Juridische Zaken van de Kamer (zie bijlage):

Wat de algemene opmerkingen betreft (punten 1 en 2) neemt de minister akte van de geformuleerde opmerkingen, maar hij zal die aanpassingen meenemen in een later ontwerp. Ofwel leiden de opmerkingen op dit moment namelijk niet naar een onduidelijkheid, ofwel treden de wijzigingen pas binnen enkele jaren in werking zodat er wat dat betreft nog voldoende tijd is. Alleen de opmerking met betrekking tot artikel 531 neemt hij wel mee; daar wordt een amendement voor ingediend.

Wat de bijzondere opmerkingen bij de artikelen betreft:

Inzake de punten 3 tot 10 van de wetgevingstechnische nota heeft de meerderheid amendementen ingediend, behalve wat de volgende opmerkingen betreft:

— de wijziging van artikel 70 van de wet van 5 juli 2022 werd niet in het wetsontwerp opgenomen omdat ze pas vanaf het aanslagjaar 2028 van kracht zal worden en ze reeds door een ander wetsontwerp zal worden gewijzigd;

— de wijziging van artikel 60 is niet meegenomen. Artikel 129/1 WIB 92 is enkel van toepassing op verkorte belastbare tijdperken. Het feit dat de verwijzing naar de vrijstelling voor pc-privéplannen pas vanaf aanslagjaar 2027 wordt opgeheven, belet de correcte toepassing van artikel 129/1 WIB 92 niet. Artikel 129/1 WIB 92 beperkt het per belastbaar tijdperk vrijstelbare bedrag in verhouding tot de duur van het belastbare tijdperk. Die beperking speelt enkel voor toekenningen die in aanmerking komen voor de vrijstelling, dus voor toekenningen tot en met 30 september 2025.

In artikel 92 en 93 gaat de minister akkoord met de schrapping van het woord “fiscale” in de Franse tekst, zodat “fraude fiscale” wordt gewijzigd in “fraude” en de Nederlandse en de Franse tekst opnieuw gelijk zijn; dit

MESDAMES, MESSIEURS,

Votre commission a examiné ce projet de loi au cours de ses réunions des 21 octobre, 4 novembre, 5 novembre, 12 novembre, 18 novembre et 25 novembre 2025.

I. — EXPOSÉ INTRODUCTIF

M. Jan Jambon, vice-premier ministre et ministre des Finances et des Pensions, chargé de la Loterie Nationale et des Institutions culturelles fédérales, apporte les précisions suivantes à la suite de la note de légistique du service Affaires juridiques de la Chambre (voir annexe):

En ce qui conserve les observations générales (points 1 et 2), le ministre prend acte, mais il intégrera ces modifications dans un projet ultérieur. Soit les points sur lesquels portent les remarques ne génèrent pas d'incertitude à ce stade, soit les modifications dont il est question n'entreront en vigueur que dans quelques années, ce qui laisse encore suffisamment de temps pour agir. Il ne reprend que l'observation relative à l'article 531. Un amendement sera présenté à cet égard.

En ce qui concerne les observations particulières relatives aux articles:

En ce qui concerne les points 3 à 10 de la note de légistique, des amendements ont été déposés par la majorité, sauf pour les remarques suivantes:

— la modification de l'article 70 de la loi du 5 juillet 2022 n'est pas intégrée car elle ne produira ses effets qu'à partir de l'exercice d'imposition 2028 et elle sera d'ailleurs déjà modifiée par un autre projet de loi;

— la modification de l'article 60 n'a pas été reprise. L'article 129/1, CIR 92, ne s'applique qu'aux périodes imposables raccourcies. Le fait que le renvoi à l'exonération pour les plans PC-privé ne soit abrogé qu'à compter de l'exercice 2027 n'empêche en rien l'application correcte de l'article 129/1, CIR 92. L'article 129/1, CIR 92 limite le montant exonéré par période imposable proportionnellement à la durée de la période imposable. Cette limitation ne s'applique qu'aux octrois éligibles à l'exonération, donc aux octrois accordés jusqu'au 30 septembre 2025.

Dans les articles 92 et 93, le ministre accepte la suppression du mot “fiscale” dans la version française, de façon à ce que “fraude fiscale” soit remplacé par “fraude” et à ce que les versions néerlandophone et

lijkt hem eerder een technische aanpassing waar geen amendement voor nodig is.

De minister kan zich evenwel volledig vinden in de vormelijke verbeteringen en taalkundige correcties, met uitzondering van de beoogde toevoeging in artikel 14. De verduidelijking dat het om hypothecaire leningen zou moeten gaan, is immers inhoudelijk niet correct, aangezien ook niet-hypothecaire leningen onder die bepaling vallen.

II. — ALGEMENE BESPREKING

A. Vragen en opmerkingen van de leden

1. Vergadering van 21 oktober 2025

De heer Lode Vereeck (VB) heeft bedenkingen bij de wijze waarop de regering voor dit ontwerp een impactanalyse verricht. Als men een maatschappelijk probleem vaststelt, kan de wetgeving hieraan sleutelen. In dit geval getuigt de oefening van weinig kwaliteit.

Vastgoedfiscaliteit

Voor de vastgoedfiscaliteit getuigt het van slecht beleid om afspraken tijdens de rit te wijzigen, ook al is het om louter budgettaire redenen.

Expats

Waarom is voor de expats het aandeel “kosten eigen aan de werkgever” zoveel hoger dan voor de eigen ingezetenen? In het jaar dat de expats naar België komen en verhuiskosten hebben, lijkt dit logisch, maar daarna is dat niet meer noodzakelijk. Als zij niet naar België willen komen omwille van de zware fiscale druk, ligt de oplossing niet in een zoveelste uitzondering via een expatstatuut.

Flexi-jobs en belastingvrije som

De heer Vereeck plaatst kanttekeningen bij de uitleg van de minister. Er rijst onduidelijkheid over de staatssteun. Er is wel degelijk een voordeel voor bedrijven die flexi-jobbers in dienst nemen, want zij moeten geen bedrijfsvoorheffing betalen. De spreker heeft kritiek op de verhoging van de belastingvrije som (18.000 euro), voorzover er discriminatie optreedt tussen voltijds werkers in een 5/5^e hoofdactiviteit en voltijds werkers

francophone du texte coïncident à nouveau. Il s'agit selon lui d'une modification technique ne nécessitant pas d'amendement.

En ce qui concerne les améliorations de forme et les corrections linguistiques, le ministre peut y souscrire entièrement, à l'exception de l'ajout prévu à l'article 14. En effet, la précision selon laquelle il devrait s'agir de prêts hypothécaires n'est pas correcte sur le fond, puisque les prêts non hypothécaires sont également visés par cette disposition.

II. — DISCUSSION GÉNÉRALE

A. Questions et observations des membres

1. Réunion du 21 octobre 2025

M. Lode Vereeck (VB) émet quelques réserves à propos de la méthode appliquée par le gouvernement pour son analyse d'impact de ce dossier. Lorsqu'un problème est constaté dans la société, la législation permet d'y remédier. En l'espèce, le travail législatif est d'une qualité médiocre.

Fiscalité immobilière

En matière de fiscalité immobilière, il n'est pas bon de changer les règles en cours de partie, même pour des raisons purement budgétaires.

Expatriés

Pourquoi la part des “frais propres à l'employeur” est-elle tellement plus élevée pour les expatriés que pour les résidents? Cela semble logique pour l'année où les expatriés arrivent en Belgique et ont des frais de déménagement, mais ce n'est plus nécessaire par la suite. S'ils ne veulent pas venir en Belgique en raison de la forte pression fiscale, la solution ne doit pas être recherchée dans un statut qui leur serait propre et qui constituerait une énième exception.

Les flexi-jobs et la quotité du revenu exemptée d'impôt

M. Vereeck émet des réserves à propos des explications fournies par le ministre. L'incertitude règne en ce qui concerne les aides d'État. Les possibilités offertes par les flexi-jobs sont effectivement avantageuses pour les entreprises, car elles ne doivent pas payer de précompte professionnel. L'intervenant critique toutefois l'augmentation de la quotité du revenu exemptée d'impôt (18.000 euros), dans la mesure où une discrimination

in een 4/5^e hoofdactiviteit en 1/5^e flexijob. Welke sectoren en type jobs worden hiermee bedoeld?

De Vlaams Belangfractie zal het voorstel echter steunen, zoals elk voorstel dat de lasten op arbeid verlaagt.

Autofiscaliteit

De impactanalyse over dit onderwerp was wel leerrijk. De analyse is er gekomen vanuit milieudoelstellingen. Het kabinet stelt dat er geen impact op milieu en gezondheid is. Kan hier meer uitleg over worden gegeven?

Onderhoudsuitkeringen (afdeling 6)

De heer Vereeck stipt aan dat dit ontwerp voor de alimentatiebetalers onrechtvaardige veranderingen omvat. Het zal niet alleen leiden tot meer onvrede, maar ook tot meer procedures voor de familierechtbanken.

CAP

De spreker vraagt aan de minister om te luisteren naar de kritiek van de oppositie. Hij kant zich tegen het amendement van de regering over de toegang van de fiscale administratie tot het CAP. Zonder vermoeden van fiscale fraude, zonder enige aanleiding zal de fiscus in de rekeningen van alle burgers kunnen kijken. Dit kan het pad effenen naar een “fiscale politiestaat”. Het systeem van proactieve datamining zonder vermoeden van fraude is van een andere aard dan het systeem dat thans van kracht is. Als er een vermoeden is van fraude, vraagt de fiscus gegevens op en verlangt hij binnen de maand een antwoord. Bij gebrek aan afdoende antwoord kan de fiscus toestemming krijgen om de gegevens in het CAP te onderzoeken. Dit ontwerp voorziet echter in een proactieve toegang tot het CAP, via datamining, zonder aanleiding en zonder vermoeden van fraude. De spreker wijst op de voorstellen van drie professoren die in het *Tijdschrift voor Fiscale Wetgeving* ertoe hebben opgeroepen om minstens een “tegenfeitelijke verklaring” te geven aan elke belastingplichtige. Dat is trouwens een Europese verplichting om burgers in alle transparantie inzicht te geven in de vraag waarom zij geselecteerd zijn, zonder dat de fiscus zijn detectiemodel hoeft vrij te geven.

De heer Kemal Bilmez (PVDA-PTB) citeert een uitspraak van de minister van Begroting in een interview van 29 september 2025 in *De Morgen*. De minister stelt vast dat in de supermarkten het aantal vaste medewerkers

apparaît entre les travailleurs à temps plein exerçant une activité principale à 5/5 et ceux à temps plein exerçant une activité principale à 4/5 et un flexi-job à 1/5. Quels sont les secteurs et les types d'emploi concernés?

Le groupe Vlaams Belang soutiendra toutefois la proposition en question, comme c'est le cas pour toute proposition visant à réduire les charges sur le travail.

Fiscalité automobile

L'analyse d'impact réalisée à ce sujet a été riche d'enseignements. Elle a été réalisée à partir d'objectifs environnementaux. Le cabinet affirme que l'impact sur l'environnement et la santé sera nul. Le membre demande de plus amples informations à ce sujet.

Rentes alimentaires (section n 6)

M. Vereeck relève que le projet de loi à l'examen prévoit d'apporter des changements injustes pour les débiteurs d'une pension alimentaire, qui entraîneront non seulement plus de mécontentement, mais aussi davantage de procédures devant les tribunaux de la famille.

Le PCC

L'intervenant demande au ministre d'écouter les critiques de l'opposition. Il rejette l'amendement du gouvernement sur l'accès au PCC accordé à l'administration fiscale. Sans aucune présomption de fraude sociale ni aucun motif, le fisc pourra consulter les relevés de comptes de tous les citoyens. Cela peut ouvrir la voie à un “État policier fiscal”. Le système de *data mining* proactif sans présomption de fraude est d'une autre nature que le système qui est en vigueur actuellement. Aujourd'hui, lorsqu'il soupçonne une fraude, le fisc demande à recevoir des données et attend une réponse dans le mois. S'il ne reçoit pas de réponse satisfaisante, il peut obtenir l'autorisation d'examiner les données dans le PCC. Le projet à l'examen prévoit toutefois un accès proactif au PCC, à travers le *data mining*, sans aucun motif ni présomption de fraude. L'intervenant se réfère aux propositions de trois professeurs qui, dans la revue *Tijdschrift voor Fiscale Wetgeving*, ont appelé à donner au moins une “explication contrefactuelle” à chaque contribuable. Une obligation européenne impose d'ailleurs d'expliquer aux citoyens, en toute transparence, pourquoi ils ont été sélectionnés, sans que le fisc ne doive pour autant divulguer son modèle de détection.

M. Kemal Bilmez (PVDA-PTB) cite les propos du ministre du Budget qui, dans une interview parue le 29 septembre 2025 dans le journal *De Morgen*, constate que les supermarchés emploient de moins en moins

daalt. Zij ruimen plaats voor flexi-jobbers of studenten, wat de sociale zekerheid ondermijnt omdat zij geen belastingen of sociale bijdragen betalen. De spreker heeft deze situatie ook ervaren toen hij jobstudent was in Delhaize.

De spreker waarschuwt voor de economische en sociale gevolgen: de vakbonden wijzen op de aanzienlijke kosten van flexi-jobs en studentenjobs voor de sociale zekerheid (respectievelijk 76 miljoen en 558 miljoen euro per jaar). Het heeft een negatieve impact op de arbeidsmarkt. Werkzoekende jongeren die voltijds willen werken, zien hun kansen verminderd door de systemen van flexibele arbeid.

Het systeem verstoort het leerproces bij jongeren: Hassan Al Hilou, de oprichter van Capital VZ2, een organisatie die in Brussel jongeren aan het werk helpt, getuigt dat makkelijk toegankelijke jobs door flexi-jobbers en studenten worden overgenomen. Hierdoor komen jongeren zonder diploma moeilijk aan werk. Niet alleen academische onderzoekers, maar ook studentenverenigingen waarschuwen voor de negatieve effecten op het schoolsucces van studenten.

De heer Bilmez vermeldt de uitbreiding van de maatregel naar kinderen van 15 jaar en toont zich bezorgd over de negatieve implicaties voor het onderwijs en de ontwikkeling van deze jongeren.

De heer Bilmez besluit dat vakbonden en wetenschappers de negatieve effecten van het systeem op de arbeidsmarkt en de jongeren hebben aangegeven. De minister van Begroting zegt zelf dat flexi-jobs de sociale zekerheid ondermijnen, en het wetsontwerp zou dit risico onderschrijven, terwijl zelfs de impactanalyse een negatief effect op gelijke kansen en sociale cohesie aangeeft.

In dit verband vraagt de heer Bilmez aan de minister van Financiën of hij akkoord gaat met de verklaringen van de minister van begroting over de ondermijnende effecten van flexi-jobs en studentenjobs en waarom een maatregel wordt voorgesteld die schadelijk is voor de jongeren, met name voor de 15-jarigen.

De heer Vincent Van Quickenborne (Open Vld) heeft van de wetgevingstechnische nota van de diensten van de Kamer kennisgenomen en wenst op een aantal punten tussen te komen:

de collaborateurs permanenten. Ceux-ci sont remplacés par des flexi-jobistes ou des étudiants, ce qui sape la sécurité sociale car ils ne paient pas d'impôts ni de cotisations sociales. L'intervenant a aussi connu cette situation lorsqu'il travaillait comme étudiant jobiste dans un magasin Delhaize.

Le député alerte sur les conséquences économiques et sociales. Les syndicats évoquent les coûts considérables des flexi-jobs et des jobs d'étudiant pour la sécurité sociale (respectivement 76 et 558 millions d'euros par an). Cette situation nuit au marché du travail. Les systèmes de travail flexible réduisent les opportunités pour les jeunes demandeurs d'emploi qui veulent travailler à temps plein.

Le système perturbe le processus d'apprentissage des jeunes: Hassan Al Hilou, fondateur de l'asbl Capital, une organisation qui aide les jeunes à trouver du travail à Bruxelles, révèle que les emplois facilement accessibles sont occupés par des flexi-jobistes et des étudiants jobistes. Les jeunes non diplômés éprouvent ainsi des difficultés à trouver un travail. Par ailleurs, des chercheurs universitaires, mais aussi des associations d'étudiants mettent en garde contre les répercussions négatives du travail étudiant sur la réussite scolaire des étudiants.

M. Bilmez évoque l'extension du travail étudiant aux jeunes à partir de 15 ans et s'inquiète de l'incidence néfaste de cette mesure sur l'enseignement et sur le développement de ces jeunes.

Il conclut en indiquant que les syndicats et les scientifiques ont mis en évidence les effets négatifs du système sur le marché de l'emploi et sur les jeunes. Le ministre du Budget lui-même affirme que les flexi-jobs sapent la sécurité sociale, et le projet de loi accepterait ce risque, alors même que l'analyse d'impact révèle une incidence négative sur l'égalité des chances et la cohésion sociale.

À cet égard, M. Bilmez demande au ministre des Finances s'il souscrit aux déclarations du ministre du Budget sur les effets nuisibles des flexi-jobs et des jobs d'étudiant. Il voudrait aussi connaître la raison pour laquelle le projet de loi prévoit une mesure qui serait préjudiciable aux jeunes, précisément aux jeunes de 15 ans.

M. Vincent Van Quickenborne (Open Vld) a pris connaissance de la note de légistique des services de la Chambre, et souhaiterait intervenir sur plusieurs points.

Flexi-jobs

De heer Vincent Van Quickenborne heeft kritiek op de beweringen van de minister van Begroting dat flexi-jobs gaten slaan in de sociale zekerheid en begroting. Volgens de minister van Begroting zou het optrekken van de limiet van de flexi-jobs van 12.000 naar 18.000 euro gaten in de begroting veroorzaken. De spreker merkt fijntjes op dat de partij van de huidige minister van Begroting al de tijd in de regering heeft gezeten en, na goedkeuring van de flexi-jobs in 2015, vervolgens in 2018, 2020 en 2022 het stelsel heeft uitgebreid. Na 10 jaar uit de minister van Begroting kritiek op de flexi-jobs. De spreker vraagt of flexi-jobs gaten in de begroting slaan en of de minister van Financiën achter het standpunt van zijn collega staat. Beschikt de minister over cijfers om die stelling te staven?

Vervolgens hekelt de spreker de inconsistente berichtgeving in de kranten. *Het Nieuwsblad* verspreidt op 7 oktober 2025 het bericht dat de Raad van State kritisch is over de uitbreiding van flexi-jobs en beweert dat het gaat om staatssteun waarvoor de Europese Commissie haar goedkeuring moet geven. *De Tijd* heeft deze berichtgeving overgenomen.

De minister van Financiën beweert daarop dat het geen staatssteun is.

De spreker wijst erop dat het advies van de Raad van State geen gewag maakt van de uitbreiding van de flexi-jobs naar alle sectoren. Het advies had het wel over de verhoging van 12.000 naar 18.000 euro.

De minister had beter gecommuniceerd dat de Raad van State over de uitbreiding naar andere sectoren geen opmerking had geformuleerd. De inconsistenties in de berichtgeving leiden tot onrust onder de sociaal secretariaten en de 230.000 mensen met een flexi-job.

Naast de vraag of flexi-jobs gaten slaan in de begroting en de sociale zekerheid, had de heer Van Quickenborne graag een stand van zaken en cijfers omtrent de verschuiving van flexi-jobs naar vaste banen.

“Aanslagjaar speciaal”

De heer Van Quickenborne heeft vragen bij de merkwaardige regeling met de benaming “aanslagjaar speciaal”, gericht op personen die slechts een deel van het jaar in België verblijven.

Les flexi-jobs

M. Vincent Van Quickenborne critique les affirmations du ministre du Budget selon lesquelles les flexi-jobs constituent un manque à gagner pour la sécurité sociale et pour le budget. Selon ce ministre, la majoration, de 12.000 à 18.000 euros, du plafond de revenus applicable aux flexi-jobs engendrera des déficits budgétaires. L'intervenant fait subtilement remarquer que le parti de l'actuel ministre du Budget a fait partie, sans interruption, de gouvernements qui, après avoir approuvé la création des flexi-jobs en 2015, ont ensuite étendu ce régime en 2018, 2020 et 2022. Aujourd'hui, le ministre du Budget critique les flexi-jobs dix ans après leur création. L'intervenant demande si les flexi-jobs engendrent effectivement un manque à gagner budgétaire, et si le ministre des Finances souscrit à la position de son collègue du Budget. Le ministre dispose-t-il de chiffres pour étayer cette affirmation?

L'intervenant poursuit en fustigeant l'incohérence des informations publiées dans la presse. Le quotidien flamand *Het Nieuwsblad* a rapporté, le 7 octobre 2025, que le Conseil d'État était critique à l'égard de l'extension du régime des flexi-jobs, et soutenait qu'il s'agissait d'une aide d'État nécessitant l'approbation de la Commission européenne. Le quotidien flamande *De Tijd* a relayé cette information.

Or, le ministre des Finances a réagi en prétendant que cette extension ne constituait pas une aide d'État.

L'intervenant souligne que l'avis du Conseil d'État ne porte pas sur l'extension des flexi-jobs à l'ensemble des secteurs, mais sur le relèvement du plafond de revenus de 12.000 à 18.000 euros.

Le ministre aurait dû mieux communiquer en soulignant que le Conseil d'État n'avait formulé aucune observation sur l'extension de ce régime à d'autres secteurs. L'incohérence des informations a suscité des inquiétudes parmi les secrétariats sociaux et les 230.000 flexi-jobistes.

Parallèlement à sa question de savoir si les flexi-jobs engendrent un manque à gagner pour le budget et pour la sécurité sociale, M. Van Quickenborne aimerait obtenir un état des lieux et des chiffres concernant la conversion de flexi-jobs en emplois fixes.

“L'exercice d'imposition spécial”

M. Van Quickenborne pose plusieurs questions à propos de l'étrange dispositif baptisé “exercice d'imposition spécial”, qui vise les personnes qui ne séjournent qu'une partie de l'année en Belgique.

De Raad van State heeft aangegeven dat de tekst in artikel 20 van het voorontwerp aangepast moet worden zodat de regeling geldt vanaf het belastbare tijdperk overeenstemmend met kalenderjaar 2025 (of een gedeelte ervan) voor bezoldigingen die in 2025 belastbaar zijn. De spreker vraagt waarom de minister de tekst niet heeft aangepast.

Hybride wagens

Het regeerakkoord van eind januari 2025 getuigde van een ambitieus plan om het bedrijfswagenpark te elektrificeren, maar na enkele maanden kondigde de regering aan om plug-inhybridewagens weer fiscaal aantrekkelijk te maken en te voorzien in een ruimere overgangperiode voor hybride wagens. De versoepeling voor hybride wagens met een fiscaal aantrekkelijk regime heeft voor gevolg dat veel bedrijven hybride wagens bestellen. Dergelijke maatregel moet evenwel de goedkeuring van Europa krijgen. Hierdoor kwam de maatregel op de helling te staan.

Deze ontwikkelingen hebben geleid tot onrust bij de personen die een hybride auto hebben aangeschaft.

De spreker pleit voor een overgangsmaatregel voor mensen die tussen eind januari en medio juni dit jaar reeds te goeder trouw een hybride auto hebben aangeschaft, zodat zij niet hun fiscale voordeel verliezen, en waarbij wordt voorzien in versnelde afschrijvingen voor bestellingen van hybride wagens die binnen een bepaalde periode zijn geplaatst.

De heer Van Quickenborne vraagt of er overleg met de Europese Commissie heeft plaatsgevonden en of zo'n overgangsmaatregel is besproken tussen eerste en tweede lezing.

Geen behoorlijke wetgeving en onduidelijkheid over de ingangsdatum

Er is onduidelijkheid over de inwerkingtreding van de ingevoerde taksen. Tussen de eerste en tweede lezing zijn enkele data gepasseerd. Het wetsontwerp noemt de "pc-privétaks" met inwerkingtreding op 30 september 2025. Op de datum van de bespreking in commissie schrijven we 21 oktober 2025. Dit lijkt niet coherent.

De Raad van State verzoekt om inwerkingtreding ná de datum van bekendmaking van de wet (niet ervoor).

In het verleden is bij de programmawet reeds geregeld dat de inwerkingtreding bij bekendmaking van de

Le Conseil d'État a indiqué que le texte de l'article 20 de l'avant-projet de loi devait être modifié de sorte que ce dispositif s'applique à partir de la période imposable correspondant à l'année civile 2025 (ou à une partie de celle-ci) pour les rémunérations imposables en 2025. L'intervenant demande pourquoi le ministre n'a pas modifié le texte en ce sens.

Véhicules hybrides

L'accord de gouvernement conclu fin janvier 2025 contenait un plan ambitieux visant à électrifier le parc des voitures de société, mais, après quelques mois, le gouvernement a annoncé sa décision de restaurer l'attractivité fiscale des voitures plug-in hybrides et de prévoir une période transitoire plus longue pour les véhicules hybrides. Cet assouplissement applicable aux véhicules hybrides au travers d'un régime fiscal avantageux a eu pour conséquence que de nombreuses entreprises ont commandé des véhicules de ce type. Mais, puisque cette mesure doit recevoir le feu vert de la Commission européenne, elle est incertaine.

Ces développements ont suscité l'inquiétude des personnes qui ont acheté une voiture hybride.

L'intervenant préconise une mesure transitoire pour les personnes ayant déjà acheté de bonne foi un véhicule hybride entre la fin janvier et la mi-juin de cette année, de manière à leur éviter de perdre leur avantage fiscal. Cette mesure prévoirait aussi des amortissements accélérés pour les commandes de véhicules hybrides passées durant une certaine période.

M. Van Quickenborne demande si une concertation a déjà eu lieu avec la Commission européenne, et si la mise en œuvre d'une mesure transitoire de cette nature a été examinée entre la première et la deuxième lecture.

Législation inadéquate et dates d'entrée en vigueur floues

Les dates d'entrée en vigueur des taxes instaurées sont floues, plusieurs dates ayant été dépassées entre la première et la deuxième lecture. Par exemple, le projet de loi à l'examen prévoyait de supprimer l'exonération fiscale du régime PC privé dès le 30 septembre 2025. Or, nous sommes aujourd'hui le 21 octobre 2025. Cela ne semble pas cohérent.

Le Conseil d'État demande de prévoir des dates d'entrée en vigueur postérieures (et non antérieures) à la date de publication de la loi.

Par le passé, il avait déjà été prévu dans la loi-programme que l'entrée en vigueur des dispositions pourrait

wet in het *Belgisch Staatsblad* kan plaatsvinden, en amendementen van de oppositie zijn toen aangenomen. Waarom kan dit hier niet worden toegepast voor de artikelen 51, 52, 59 en 82, en waarom zijn geen amendementen ingediend om de ingangsdatum te koppelen aan de bekendmaking (en niet aan voorliggende data zoals 30 augustus en 30 september 2025)?

CAP en datamining (screening van bankrekeningen en betalingsverkeer)

Voorts plaatst de heer Van Quickenborne kanttekeningen bij de maatregelen van de regering met betrekking tot het Centraal Aanspreekpunt (CAP) van de Nationale Bank in het wetsontwerp. Dit betreft de mogelijkheid tot het grootschalige en geautomatiseerde gebruik van gegevens via datamining om fraude op te sporen. Dit gebruik van gegevens via datamining heeft een zware maatschappelijke impact en een impact op de persoonlijke levenssfeer. Op Europees niveau is er sinds 2022 discussie over *chat control*, waarbij overheden toegang zouden hebben tot persoonlijke berichten. Ook dit impliceert een uitgebreide screening en profilering. De spreker onderkent een patroon waarin de privacy van burgers van geen tel is, waardoor iedereen die communiceert, voorschrijft of een bankrekening heeft, per definitie als verdachte wordt beschouwd.

De spreker heeft bedenkingen bij de parlementaire weg die de regeringsamendementen hebben afgelegd, die hij ook reeds tijdens de bespreking op 23 september 2025 heeft aangehaald.

Er zijn intussen binnen de meerderheid verdeelde stemmen gehoord. Enkelen maken zich zorgen over privacy, zoals MR- kamerlid Michel, die op 28 mei 2025 in plenaire vergadering een kritische vraag heeft gesteld naar aanleiding van een vernietigend advies van de Gegevensbeschermingsautoriteit.

Het merkwaardige verloop waarbij regeringsamendementen over het CAP en de datamining worden ingediend, teruggetrokken of gewijzigd, lijkt nogal grillig. Er is weinig transparantie en verantwoording van de zijde van de regering en een debat en parlementaire input blijven uit.

De heer Van Quickenborne roept op tot een breed debat, hoorzittingen en duidelijke uitleg over het CAP en de datamining, inclusief publieke betrokkenheid en

avoir lieu au moment de la publication de la loi au *Moniteur belge*, et les amendements de l'opposition avaient alors été adoptés. Pourquoi cette méthode ne pourrait-elle pas être reproduite pour les articles 51, 52, 59 et 82? Et pourquoi aucun amendement n'a-t-il été présenté pour faire coïncider la date d'entrée en vigueur et la date de publication (et ne pas prévoir de dates d'entrée en vigueur antérieures, comme le 30 août ou le 30 septembre 2025)?

PCC et data mining (contrôle des comptes bancaires et des paiements)

M. Van Quickenborne émet en outre des réserves à propos des mesures que le gouvernement prévoit dans le projet de loi à l'examen au sujet du Point de contact central (PCC) de la Banque nationale. Elles concernent la possibilité d'utiliser des données à grande échelle et de manière automatisée à des fins de *data mining* dans le but de détecter des fraudes. Cette utilisation des données à des fins de *data mining* impactera considérablement la société et la vie privée. Au niveau européen, on débat depuis 2022 du contrôle des conversations privées (*chat control*), qui permettrait aux autorités d'avoir accès aux messages personnels, ce qui implique également un contrôle et un profilage étendus. L'intervenant y voit une tendance à ne pas tenir compte de la vie privée des citoyens, de sorte que toute personne qui communique des informations, établit des prescriptions ou possède un compte bancaire sera, par définition, considérée comme suspecte.

L'intervenant émet quelques critiques concernant le parcours parlementaire que les amendements du gouvernement ont suivi, parcours qu'il a également déjà évoqué le 23 septembre 2025 au cours de la discussion.

Dans l'intervalle, des voix dissonantes se sont fait entendre au sein de la majorité. Quelques-uns de ses membres s'inquiètent du respect de la vie privée. Il s'agit notamment de M. Michel, député du groupe MR, qui a posé une question critique en séance plénière le 28 mai 2025 à la suite de l'avis accablant rendu par l'Autorité de protection des données.

Le parcours des amendements du gouvernement relatifs au PCC et au *data mining*, qui ont été tour à tour déposés, retirés ou modifiés, semble plutôt insolite. Le gouvernement ne fait guère preuve de transparence et ne se justifie pas davantage. Il ne laisse en outre guère de place à un débat et un apport parlementaires.

M. Van Quickenborne appelle à organiser un large débat, à procéder à des auditions et à apporter des explications claires au sujet du PCC et du *data mining*,

politieke standpunten, alvorens dergelijke ingrijpende maatregelen te implementeren.

De spreker beklemtoont dat de maatregelen inzake het CAP en datamining raken aan het privéleven. Gegevens over sparen en uitgaven, bankgegevens zijn gedragsprofielen. Zij brengen aan het licht wie iemand is, wat hij leest en koopt, waarheen hij reist, welke doelen hij steunt en hoeveel hij spaart. Grootschalige datamining betekent dat de overheid niet wacht op een aanwijzing, maar actief zoekt in het dagelijks gedrag van de burger.

Het legaliteitsbeginsel komt hierbij onder druk te staan. Datamining verschuift de aanleiding van wettelijke toegang. De gegevens, drempels, doeleinden, bewaartermijnen en burgerrechten moeten nauwkeurig bij de wet bepaald zijn.

De spreker hekelt het schouwspel waarbij allerlei amendementen de revue passeerden. Het was een schouwspel van “procedurele mist”.

De heer Van Quickenborne waarschuwt dat de privacy, de legaliteit en de proportionaliteit op het spel staan. De massale screening van rekeningen vormt een risico voor het privéleven. Ofwel is er een doelbewuste, beperkte toetsing met duidelijke grenzen, ofwel een massale data-analyse met weinig waarborgen. De evenredigheid is zoek als men voor het navlooiën van enkele tientallen dossiers een zware inbreuk pleegt op de gegevens van miljoenen mensen.

Geen enkel algoritme mag definitief beslissen. Menselijke toetsing moet vroeg plaatsvinden en transparant zijn. Zonder traceerbare motivering is elke controle potentieel willekeurig. Er is behoefte aan duidelijke parameterkennis en alternatieven.

We moeten voorkomen dat iedere burger als een potentiële verdachte wordt aangemerkt. De spreker verwijst naar de toeslagenaffaire in Nederland, waar algoritmes voor vele burgers ernstige negatieve gevolgen tot gevolg hadden. Gaan wij dezelfde weg op? Er wordt gewaarschuwd voor de risico's van deze methoden.

Net zoals het debat over *chat control* is er nood aan een publiek debat over de financiële variant van *chat control* en over het CAP en datamining.

en ce compris l'implication publique et les points de vue politiques, avant de mettre en œuvre de telles mesures radicales.

L'intervenant souligne que les mesures relatives au PCC et au *data mining* touchent la vie privée. Les données concernant l'épargne et les dépenses ainsi que les données bancaires sont des profils comportementaux. Elles révèlent la véritable nature d'une personne, ce qu'elle lit et achète, où elle voyage, quels sont les œuvres qu'elle soutient et le montant de son épargne. Le *data mining* à grande échelle signifie que les autorités n'attendent pas une indication, mais effectuent activement des recherches dans le comportement quotidien du citoyen.

Ces pratiques mettent à mal le principe de légalité. Le *data mining* déplace le motif permettant d'accéder légalement à la vie privée. Les données, les seuils d'accessibilité, les finalités, les délais de conservation et les droits civils doivent être définis avec précision par la loi.

L'intervenant critique le spectacle au cours duquel toutes sortes d'amendements ont été passés en revue et le qualifie de “brouillard procédural”.

M. Van Quickenborne souligne que les enjeux sont la vie privée, la légalité et la proportionnalité. Le contrôle massif des comptes bancaires constitue une menace pour la vie privée. Soit il s'agit d'un contrôle ciblé et restreint, assorti de limites claires, soit il s'agit d'une analyse massive de données offrant peu de garanties. Il n'est plus question de proportionnalité lorsque l'on porte gravement atteinte aux données de millions de personnes afin de passer au crible quelques dizaines de dossiers.

Aucun algorithme ne peut prendre de décision définitive. Le contrôle humain doit intervenir à un stade précoce et dans la transparence. Sans justification traçable, tout contrôle est potentiellement arbitraire. Il est nécessaire de connaître clairement les paramètres et de disposer d'alternatives.

Il faut empêcher que chaque citoyen soit considéré comme un suspect potentiel. L'intervenant évoque l'affaire des allocations aux Pays-Bas, où les algorithmes ont eu de graves répercussions négatives pour de nombreux citoyens. Suivrons-nous la même voie? Des mises en garde sont formulées au sujet des risques que présentent ces méthodes.

Tout comme c'est le cas dans le débat concernant *chat control*, un débat public est nécessaire au sujet de sa variante financière ainsi qu'à propos du PCC et du *data mining*.

Zonder publiek debat en duidelijke grenzen kunnen zulke instrumenten misbruikt worden. De heer Van Quickenborne stelt een debat voor over het CAP en de datamining, en dit zou in vier stappen kunnen verlopen:

— Eerst legt men de feiten op tafel: Wat zit er nu in het CAP? Wat verandert er door de regeringsamendementen? Vragen worden gesteld over technische koppelingen, query's, drempels, sampling, frequentie, en het meten van de betrouwbaarheid (valse positieven/negatieven)?

— Vervolgens legt men de methoden bloot: Hoe werkt datamining bij de fiscus (los van het CAP)? Wat is een "DAM"-fiche? Wie keurt het goed en wat zijn de bewaartijden van de analysetabellen?

— Ten derde is er oog voor de juridische controle: aandacht voor rechtsinstrumenten en grondrechten (art. 22 GW, de algemene verordening gegevensbescherming, het EVRM, de proportionaliteit en transparantie).

— Het vierde aandachtspunt, "Governance en tegenmacht", is tevens het sluitstuk: Wie houdt toezicht? Wat zijn de rechten van de Kamer? Jaarlijkse openbare hoorzittingen, de publicatie van drempels en evaluaties volgen dit alles op.

Het doel is een systeem dat efficiëntie biedt zonder afbreuk te doen aan de grondrechten; efficiëntie moet voortkomen uit goed ontworpen rechtssystemen.

De spreker waarschuwt voor een "*money control*" / "*cash control*"-systeem dat bankrekeningen, saldi en financiële contracten kan screenen. De huidige tekst kent geen beperkingen en zet de persoonlijke levenssfeer op het spel. Het gaat niet enkel om ernstige fiscale fraude. Hij geeft het voorbeeld van een jongere die, na verkoop van een DAX, 3000 euro extra inkomsten ontvangt boven op zijn loon. Omdat die mogelijk niet rechtmatig zijn, krijgt de fiscus argwaan en vraagt om uitleg. De voorgestelde wettekst laat geen expliciete beperking tot "ernstige en georganiseerde fraude" zien; daarom kan iedereen in het kader van alle mogelijke geldstromen worden onderzocht.

Faute de débat public et de limites claires, ces instruments pourront être utilisés à mauvais escient. M. Van Quickenborne propose un débat sur le PCC et le *data mining* qui pourrait se dérouler en quatre étapes:

— Premièrement, les faits sont exposés. En quoi consiste actuellement le PCC? Quels sont les changements apportés par les amendements du gouvernement? Des questions sont posées concernant les interconnexions techniques, les requêtes, les seuils, l'échantillonnage, la fréquence et la mesure de la fiabilité (faux positifs/négatifs)?

— Ensuite, les méthodes sont expliquées: Comment fonctionne le *data mining* au sein du fisc (indépendamment du PCC)? Qu'est-ce qu'une "fiche DAM"? Qui l'approuve et quels sont les délais de conservation des tableaux d'analyse?

— Troisièmement, on se soucie du contrôle juridique: attention portée aux instruments juridiques et aux droits fondamentaux (l'art. 22 de la Constitution, le Règlement général sur la protection des données, la CEDH, la proportionnalité et la transparence).

— Pour conclure, le quatrième point, "Gouvernance et contre-pouvoir": qui exerce la surveillance? Quels sont les droits de la Chambre? Des auditions publiques annuelles, la publication des seuils et des évaluations auront-elles lieu par la suite?

L'objectif est de mettre en place un système efficace sans porter atteinte aux droits fondamentaux. Or, pour être efficace, le système doit reposer sur des dispositifs juridiques bien ficelés.

L'intervenant met en garde contre l'instauration d'un système de contrôle des flux financiers et des espèces qui permettra de passer au crible les comptes bancaires, les soldes et les contrats financiers. Dans sa formulation actuelle, le texte ne prévoit aucune restriction et met en péril la vie privée. Le système envisagé ne se limitera pas à la fraude fiscale grave. L'intervenant donne l'exemple d'un jeune qui touche 3000 euros de revenus en plus de son salaire après avoir vendu sa mobylette Dax. Comme ces revenus pourraient être illicites, le fisc a des soupçons et demande des renseignements. Le projet de loi à l'examen ne prévoyant pas explicitement de limiter ce système à la "fraude grave et organisée", tous les flux financiers pourront être contrôlés, quel que soit le détenteur.

De spreker verwijt de meerderheid dat zij geen beperkingen wil voorzien en stelt dat sommige fracties (zoals de Vooruit-fractie) een dergelijk systeem zelfs wensen.

De spreker uit kritiek op het feit dat de voorgestelde regeling toezicht uitbouwt, dat niet enkel gericht is op georganiseerde en ernstige fraude, maar op een brede surveillance van iedereen. Dit blijkt uit de lezing van de tekst ("inbreuk op een wet of reglementering").

Hij stelt dat afdwinging in wetten moet liggen en waarschuwt dat zonder wettelijke detailbepalingen de manoeuvreerruimte voor de fiscus te ver dreigt te gaan. De controles moeten duidelijke grenzen hebben. De ervaring met *chat control* heeft geleerd dat men niet lichtzinnig mag morrelen aan vertrouwelijke gegevens.

Men dient een regeling uit te werken die streng en effectief is, zonder onrechtvaardig te worden. Men kan modern zijn zonder roekeloos te zijn. Men moet voorrang geven aan de logica en de rechtsstaat.

Het stoort de heer Van Quickenborne dat "data-mining" een onderdeel wordt van de "wet houdende diverse bepalingen". Deze materie verdient een apart wetsontwerp met een degelijke memorie van toelichting en hoorzittingen.

De heer Van Quickenborne verwondert zich over de stilte die over dit onderwerp heerst, zowel bij de fracties in het Parlement, als in de pers.

Het CAP dreigt in de praktijk het pad te effenen voor een brede screening van miljoenen mensen. Het CAP, dat oorspronkelijk tegen fraude gericht was, zou nu ook worden ingezet voor controles die niets met fraude te maken hebben, mogelijk leidend tot een vermogenskadaster.

De GBA (Gegevensbeschermingsautoriteit) heeft gezegd dat datamining transparantie en gerichte risico-analyses vereist, maar de regering negeert in de wetteksten, na dit advies van de GBA, die transparantieplicht.

In een recent artikel van *Het Laatste Nieuws* wordt het scenario voorspeld dat de fiscus in de toekomst proactief bank-, beleggings- en verzekeringsgegevens gaat doorzoeken met slimme software om opvallende patronen te detecteren, zelfs zonder concreet vermoeden van fraude. Waar eindigt dit? Deze voortdurende monitoring van rekeningen en financiële producten zou

L'intervenant reproche à la majorité de refuser ces restrictions et ajoute que certains groupes (notamment Vooruit) sont même favorables à l'instauration de ce système.

Il critique en outre le fait que le dispositif proposé tende à renforcer les contrôles, qu'il ne se limite pas à la fraude grave et organisée, mais qu'il vise au contraire une surveillance généralisée. Tel est ce qui ressort de la lecture du texte ("infraction à une loi ou à une réglementation").

Le membre indique que toute mesure coercitive doit être inscrite dans la loi et il prévient qu'en l'absence de dispositions légales détaillées, le fisc risque de disposer d'une trop grande marge de manœuvre. Les contrôles doivent être clairement délimités. L'expérience tirée de "*chat control*" nous a appris qu'il ne faut pas manipuler à la légère des données confidentielles.

Il convient d'élaborer un dispositif qui soit strict et efficace, sans pour autant être injuste. On peut être moderne sans faire preuve d'imprudence. La logique et l'état de droit doivent primer.

M. Van Quickenborne déplore que la question du *data mining* fasse partie intégrante de la loi portant des dispositions diverses. Cette matière mérite en effet un projet de loi à part entière, ainsi qu'un exposé des motifs et des auditions dignes de ce nom.

Il s'étonne du silence qui plane autour de cette question, tant au sein des groupes au Parlement que dans la presse.

Le PCC risque en pratique d'ouvrir la voie à des contrôles à grande échelle de millions de personnes. Initialement destiné à lutter contre la fraude, cet instrument serait désormais également utilisé pour mener des contrôles qui ne seraient nullement liés à la fraude, ce qui pourrait conduire à la création d'un cadastre des fortunes.

L'APD (Autorité de protection des données) a déclaré que le *data mining* exigeait une certaine transparence et des analyses de risques ciblées, mais le gouvernement fait fi de cette obligation de transparence dans les textes de loi, en dépit de l'avis rendu par l'APD.

Dans un article récent, *Het Laatste Nieuws* prédit que, dans le futur, le fisc épluchera de manière proactive les données bancaires, d'investissement et d'assurance à l'aide de logiciels intelligents afin de détecter les comportements qui sortent de l'ordinaire, même en l'absence de soupçons concrets de fraude. Où ces contrôles s'arrêteront-ils? Cette surveillance en continu

kunnen worden uitgebreid naar effecten- en cryptorekeningen. Het gaat om uiterst gevoelige gegevens die preventief worden doorzocht, aldus de GBA. Dit alles kan de deur openen naar een vermogenskadaster, waarbij persoonsgegevens gefaseerd van “anoniem” (in eerste instantie) naar “volledig open” (in tweede instantie) kunnen gaan en ambtenaren worden betrokken bij de beoordeling naast het algoritme.

2. Vergadering van 4 november 2025

De heer Vincent Van Quickenborne (Open Vld) vervolgt zijn tussenkomst met het debat over de zogenaamde “money control”-wetgeving en de relatief geringe aandacht daarvoor in de pers. In *De Tijd* verscheen op 28 mei 2025 wel een artikel met de titel “regering moet privacy-debat voeren”, waarin de heer Pieter Blomme, adjunct-hoofdredacteur, een pleidooi houdt voor een debat naar aanleiding van de voorliggende plannen.

De spreker citeert enkele passages uit het opiniestuk:

“De Gegevensbeschermingsautoriteit (GBA), zoals de privacycommissie tegenwoordig heet, schiet de plannen van de regering-De Wever af om datamining toe te passen op het Centraal Aanspreekpunt (CAP) [...]. De instelling oordeelt dat de plannen een te grote inbreuk zijn op onze privacy.

Het CAP bestaat al langer in de schoot van de Nationale Bank. Bij vermoedens van fraude kan dat worden geraadpleegd door hoge ambtenaren bij de fiscus.

Maar als de plannen van de regering doorgaan – het advies van de GBA is niet bindend – krijgt een kransje fiscale ambtenaren veel meer macht. De databank zou gebruikt kunnen worden voor anonieme data-analyse. Als op basis van die datamining een vermoeden van fraude naar boven komt, zou een ambtenaar worden gewaarschuwd. In plaats van een reactief instrument wordt het dus een proactief instrument.”

Verder luidt het:

“Het past in het opvoeren van de strijd tegen fiscale fraude. In een land met de hoogste belastingdruk op arbeid ter wereld is het geen overbodige luxe daarop in te zetten. Als het kan helpen die torenhoge belastingdruk te verlagen, is het logisch dat wordt nagedacht over creatieve manieren om fraude harder aan te pakken.

des comptes et des produits financiers pourrait s'étendre aux comptes-titres et aux comptes de cryptomonnaies. L'APD indique que des données extrêmement sensibles seront examinées à titre préventif. Ce dispositif risque d'ouvrir la voie à un cadastre des fortunes dans lequel les données à caractère personnel pourraient passer progressivement du statut “anonyme” (dans un premier temps) au statut “entièrement public” (dans un second temps). Des fonctionnaires seraient chargés de leur évaluation parallèlement à l'algorithme.

2. Réunion du 4 novembre 2025

M. Van Quickenborne (Open Vld) poursuit son intervention en abordant la question de la législation visant à contrôler les flux financiers (“money control”) et l'intérêt plutôt limité témoigné par la presse à cet égard. Un article intitulé *regering moet privacydebat voeren* (le gouvernement doit débattre sur la protection de la vie privée) est certes paru dans *De Tijd* le 28 mai 2025. M. Pieter Blomme, rédacteur en chef adjoint, y demandait un débat sur les projets existants en la matière.

L'intervenant cite quelques passages de cette tribune:

“L'Autorité de protection des données (APD), nouveau nom de la commission de la protection de la vie privée, tire à boulets rouges sur les projets du gouvernement De Wever visant à appliquer des techniques de *data mining* au Point de contact central (PCC) [...]. L'institution estime que le projet implique une violation trop grave de notre vie privée.

Voilà un certain temps déjà que le PCC a été créé dans le giron de la Banque nationale et que les hauts fonctionnaires du fisc peuvent le consulter en cas de suspicion de fraude.

Or, si le gouvernement maintient son projet (l'avis de l'APD n'étant pas contraignant), un petit cercle de fonctionnaires fiscaux vont voir leur pouvoir s'accroître considérablement. La banque de données pourrait être utilisée pour des analyses de données anonymisées. Si ce procédé révèle une suspicion de fraude, un fonctionnaire sera alors averti. Le fisc passe donc d'une méthode de travail réactive à une stratégie proactive.”

L'article continue comme suit:

“Ces mesures s'inscrivent dans l'intensification de la lutte contre la fraude fiscale. Dans le pays où le travail est le plus taxé au monde, ce n'est pas un luxe d'investir dans la lutte contre la fraude fiscale.

In een land met de hoogste belastingdruk op arbeid ter wereld is het geen overbodige luxe in te zetten op de strijd tegen fiscale fraude. Alleen: schiet men nu niet met een kanon op een mug?

Maar er is wel een debat nodig over de proportionaliteit van de instrumenten die worden ingezet. Schiet men niet met een kanon op een mug? Is met deze maatregel de privacy voldoende gewaarborgd? Moet de belastingplichtige niet eerst bevraagd worden alvorens toegang te verlenen tot het CAP? Het zijn vragen waarover op zijn minst een politiek debat noodzakelijk is.

Dat debat is er nauwelijks.”

De heer Van Quickenborne stelt vast dat er in deze commissie weliswaar over het thema gediscussieerd kan worden, maar dat er – behalve de inbreng van de heer Lode Vereeck (VB) – weinig animo bestaat voor deelname aan een echt debat.

De journalist van *De Tijd* besluit zijn opinie als volgt:

“Want onze privacy staat meer dan ooit onder druk. We leven in tijden waar niets meer veilig is voor de buitenwereld en waar nauwelijks nog belang wordt gehecht aan privacy. Via lekken worden vertrouwelijke gegevens te grabbel gegoooid of komen persoonsgegevens bij de verkeerde personen terecht en via hackers of phishing wordt onschuldige burgers geld afgetroggeld.

Daarom is het wenselijk dat een regering die zulke verregaande ingrepen wil doorvoeren die zou kaderen binnen een brede hervorming rond financiële transparantie.”

De regering ondermijnt echter de privacy door de manier waarop ze de plannen wil invoeren. In het wetsontwerp worden tal van maatregelen gebundeld die in één keer, vaak geruisloos, door het Parlement worden gejaagd. Het zou nochtans vanzelfsprekend moeten zijn dat zulke plannen met het vergrootglas worden bekeken, aldus het voornoemde artikel in *De Tijd*. De spreker is dan ook van plan om de voorliggende maatregel grondig tegen het licht te houden en de bescherming van de privacy voorop te stellen, want dat is de taak van parlementsleden.

In dit verband kan worden verwezen naar een diepgaand debat in het Europees Parlement dat er recent toe geleid heeft dat *chat control* van tafel is. Met dat systeem zou de communicatie van burgers gecontroleerd worden,

Si cela peut aider à réduire cette charge fiscale colossale, il est logique d'envisager des manières créatives de lutter plus fermement contre la fraude.

Mais ne serions-nous pas en train de tuer une mouche avec un canon? Un débat s'impose sur la proportionnalité des outils employés. Faut-il vraiment sortir l'artillerie lourde? Cette mesure n'entrave-t-elle pas trop la protection de la vie privée? Ne faudrait-il pas obtenir le consentement du contribuable avant d'autoriser l'accès au PCC? Toutes ces questions demandent, à tout le moins, un débat politique.

Or, ce débat est quasiment inexistant.”

M. Van Quickenborne note que, si la commission peut certes discuter du sujet, il constate – à l'exception de l'intervention de M. Lode Vereeck (VB) – peu d'enthousiasme pour participer à un véritable débat.

Le journaliste conclut comme suit sa tribune dans *De Tijd*:

“C'est que notre vie privée est plus que jamais remise en question. Nous vivons une époque où rien n'est plus à l'abri du regard extérieur et où le respect de la vie privée n'intéresse plus grand monde. Les fuites de données jettent nos informations confidentielles en pâture et les données à caractère personnel finissent entre de mauvaises mains. D'innocents citoyens sont alors extorqués par le piratage informatique et autre hameçonnage.

C'est pourquoi un gouvernement qui entend prendre des mesures aussi radicales aurait tout intérêt à les inscrire dans une réforme plus vaste de la transparence financière.”

Cependant, par la manière dont il entend mettre ses plans en œuvre, le gouvernement porte préjudice à la vie privée. Le projet de loi amalgame toute une série de mesures et les expédie en une seule fois pour approbation au Parlement, souvent en toute discrétion. D'après l'article du *Tijd*, ces projets mériteraient pourtant d'être analysés à la loupe et l'intervenant a bien l'intention de le faire, en gardant à l'esprit l'importance de la protection de la vie privée. Tel est en effet le rôle des députés.

Le membre fait le lien avec un débat de fond ayant récemment eu lieu au Parlement européen, qui a fini par avoir raison de *chat control*. Ce système visait la surveillance des communications des citoyens, tout

net zoals de Belgische regering dat voor betalingen wil invoeren. Dankzij grondige discussies in het Europees Parlement en vooral het verzet van talloze burgers tegen een dergelijke aanslag op hun privacy, kon *chat control* ten grave worden gedragen. De commissie voor Financiën en Begroting dient hetzelfde doel na te streven voor de voorliggende wetgeving die de spreker "*money control*" heeft gedoopt.

— *Houding van de minister van Financiën*

Het valt de heer Van Quickenborne op dat de minister zijn wetsontwerp en amendementen op dit punt met weinig animo verdedigt. Eerder dan uit overtuiging lijkt hij deze maatregel voor te stellen omwille van gemaakte politieke afspraken. In de antwoorden van de minister is tot nu toe voornamelijk een soort managementtaal te horen, waarbij het gaat over modernisering, harmonisatie en *data driven Control*. Alles zou binnen een wettelijk kader plaatsvinden en onder toezicht staan van de Gegevensbeschermingsautoriteit (GBA). Toch blijkt uit zijn toon dat hij er zelf niet in gelooft. Het is dan ook geen dossier dat er op initiatief van de minister komt. De meerwaardebelasting wordt ondanks alle tekortkomingen nog enigszins geloofwaardig verdedigd, maar bij de voorliggende maatregel is dat niet het geval en blijft zijn toelichting beperkt tot het herhalen van de verantwoording bij de amendementen.

De minister is in dit dossier eerder een toeschouwer dan een initiatiefnemer. Dat maakt de situatie des te ernstiger. Wie zal immers de verantwoordelijkheid dragen indien er iets verkeerd loopt en burgers ten onrechte worden gebrandmerkt als fraudeur? De spreker verwijst naar de gelijkaardige toeslagenaffaire in Nederland.

Een fiscale controle is behoorlijk intrusief. Stel dat uit het systeem tal van vals positieve dossiers komen die achteraf onterecht geselecteerd bleken te zijn, wie zal dan de schade vergoeden ten aanzien van de betrokkenen? Zal de minister van Financiën de politieke verantwoordelijkheid opnemen?

— *Het belang van een uitvoerig parlementair debat*

De spreker heeft in deze commissie meermaals gevraagd naar de parameters van de modellen die de minister wettelijk wil verankeren. Het antwoord luidde steeds dat deze informatie geheim is. Er konden geen details, cijfers of een beschrijving van de foutenmarge verstrekt worden. Wat is dan nog de taak en de rol van het Parlement? Als de volksvertegenwoordiging zwijgt, wordt het slechts een instrument van de administratie.

comme le gouvernement belge prévoit de le faire pour leurs paiements. Grâce à un débat parlementaire approfondi et, surtout, à l'opposition de nombreux citoyens contre une telle atteinte à leur vie privée, ce projet de *chat control* est finalement définitivement enterré. La commission des Finances et du Budget doit poursuivre le même objectif concernant la législation à l'examen, baptisée "*money control*" par l'intervenant.

— *Attitude du ministre des Finances*

M. Van Quickenborne est frappé par le peu d'enthousiasme dont fait preuve le ministre pour défendre son projet de loi et ses amendements sur ce point. Le ministre semble proposer cette mesure, non pas par conviction, mais pour respecter les accords politiques conclus. Dans ses réponses, ce dernier utilise, jusqu'à présent, essentiellement un jargon managérial dans lequel il est question de modernisation, d'harmonisation et de *data driven Control*, le tout devant s'opérer dans un cadre légal sous le contrôle de l'Autorité de protection des données (APD). Le ton du ministre révèle toutefois qu'il n'y croit pas lui-même. Il ne s'agit donc pas d'un dossier examiné à l'initiative du ministre. Malgré toutes les lacunes, la taxe sur les plus-values est encore défendue avec une certaine crédibilité, ce qui n'est toutefois pas le cas de la mesure à l'examen dont l'explication se limite à répéter la justification des amendements.

Dans ce dossier, le ministre est davantage spectateur qu'initiateur, ce qui aggrave d'autant plus la situation. Qui assumera, en effet, la responsabilité si des problèmes surviennent et que des citoyens sont injustement désignés comme fraudeurs? L'intervenant renvoie à l'affaire similaire des allocations familiales aux Pays-Bas.

Un contrôle fiscal est relativement intrusif. En supposant que le système mette au jour de nombreux dossiers erronément positifs qui par la suite s'avèreraient avoir été sélectionnés injustement, qui indemniserait le dommage subi par les intéressés? Le ministre des Finances en assumera-t-il la responsabilité politique?

— *L'importance d'un débat parlementaire approfondi*

L'intervenant a demandé, à plusieurs reprises au sein de cette commission, que le ministre précise les paramètres des modèles qu'il souhaite ancrer dans la loi. Il lui a été systématiquement répondu que ces informations étaient secrètes. Aucun détail, aucun chiffre ou description de la marge d'erreur ne pouvait être fourni. Quelle mission et quel rôle reste-t-il au Parlement dans ce cas? Si la représentation populaire se tait, le Parlement ne sera plus qu'un instrument de l'administration.

Het is de bedoeling van de heer Van Quickenborne om elk parlements lid de draagwijdte van deze maatregel te doen inzien, zodat niemand achteraf kan beweren dat het slechts een detail was. Men kan de burger niet aanmanen tot fiscale transparantie en tegelijk fiscale en bestuurlijke duisternis aanvaarden.

Om die reden zal de spreker uitvoerig ingaan op de gegevens waarover het CAP precies beschikt, het technisch functioneren van datamining, welke datasets er worden gekoppeld, wie de toegang beheert, welke drempels gelden voor selectie en waarom dit veel weg heeft van de toeslagenaffaire in Nederland. Het is een kwestie van tijd voor het systeem problemen zal opleveren. Pas wanneer men dit alles begrijpt, kan een weloverwogen stem worden uitgebracht. Democratie betekent immers meer dan het volgen van een procedure.

Meningsverschillen mogen dan vanzelfsprekend zijn in een Parlement, maar het is betreurenswaardig dat er gestemd wordt in onwetendheid. De heer Van Quickenborne schat dat het overgrote deel van de commissieleden niet goed begrijpt wat er precies voorligt. Verschillende fracties hullen zich in stilte; onduidelijkheid over hun standpunt is troef. N-VA kantte zich bijvoorbeeld tegen *chat control* op basis van privacy-argumenten, maar heeft plots geen bezwaar als het over betalingsgegevens gaat. Hetzelfde geldt voor Vooruit. Enkel de heer Mathieu Michel (MR) uitte zijn twijfels in een aantal vragen aan de minister, waarop geen antwoorden kwamen.

De vergelijking met het Europees debat over *chat control* is relevant. Tientallen leden van het Europees Parlement hebben zich samen met academici en experts gebogen over de essentiële vraag hoe ver men kan gaan in de Controle van communicatie zonder de essentie van privacy te vernietigen. Het Europese Parlement organiseerde hoorzittingen, in verschillende kranten verschenen opiniestukken, de Europese toezichthouder bracht adviezen uit, mensenrechtenorganisaties gaven waarschuwingen en cryptografen kwamen met technische analyses. De heer Bart Preneel, professor aan de KU Leuven, was één van de eersten die waarschuwde voor *chat control* en hij heeft daarin gelijk gekregen.

De maatschappelijke discussie over *chat control* was bijwijlen chaotisch en intens, maar was wel democratisch. Iedereen wist wat er op tafel lag. De uiteindelijke uitkomst, het afvoeren van *chat control*, is er gekomen na een grondig debat.

M. Van Quickenborne entend faire comprendre à chaque député la portée de cette mesure, afin que personne ne puisse affirmer *a posteriori* qu'il ne s'agissait que d'un détail. On ne peut sommer les citoyens de faire preuve de transparence fiscale tout en acceptant l'opacité fiscale et administrative.

L'intervenant abordera dès lors en détail les données dont dispose précisément le PCC, le fonctionnement technique du *data mining*, les ensembles de données qui y sont associés; il précisera qui en gère l'accès, les seuils applicables en matière de sélection et pourquoi ce dossier ressemble autant à l'affaire des allocations familiales aux Pays-Bas. Le système posera des problèmes: c'est juste une question de temps. Ce n'est que lorsqu'on aura compris tous les tenants et les aboutissants qu'on pourra voter en connaissance de cause. En effet, la démocratie ne se résume pas à suivre une procédure.

Il va de soi que les avis divergent au sein d'un Parlement, mais il est regrettable que des députés émettent un vote non éclairé. M. Van Quickenborne considère que le dossier à l'examen est mal compris par une écrasante majorité des membres de la commission. Plusieurs groupes politiques se retranchent dans le mutisme; le flou est la règle en ce qui concerne leur point de vue. La N-VA s'est par exemple opposée à *chat control* en faisant valoir des arguments sur la protection de la vie privée mais ne voit soudain rien à redire lorsqu'il s'agit des données de paiement. Il en va de même de Vooruit. Seul M. Mathieu Michel (MR) a exprimé ses doutes dans une série de questions au ministre, qui sont restées sans réponse.

La comparaison avec le débat européen concernant *chat control* est pertinente. Des dizaines de députés européens se sont penchés, aux côtés d'universitaires et d'experts, sur la question essentielle de savoir jusqu'où il est possible d'aller dans le contrôle des communications sans anéantir l'essence même de la protection de la vie privée. Le Parlement européen a organisé des auditions, des articles d'opinion ont été publiés dans différents journaux, le contrôleur européen de la protection des données a rendu des avis, les organisations de défense des droits de l'homme ont lancé des avertissements et les cryptographes ont présenté des analyses techniques. M. Bart Preneel, professeur à la KU Leuven, a été l'un des premiers à alerter contre *chat control* et les faits lui ont donné raison.

Bien que le débat de société au sujet de *chat control* ait parfois été chaotique et intense, il a été démocratique. Tout le monde connaissait l'enjeu. Le résultat final, à savoir l'abandon du projet "*chat control*", est le fruit d'un débat approfondi.

De spreker betreurt dat de regering in België exact hetzelfde wenst door te voeren in het financiële domein, maar dan zonder enig debat, hoorzitting, maatschappelijke discussie of analyse. Indien *chat control* op dezelfde wijze was ingevoerd, met ingetrokken en opnieuw ingediende amendementen, dan was het protest niet te overzien geweest. Toch passeert de voorliggende maatregel in deze commissie zonder veel ruchtbaarheid.

Ook het Federaal Instituut voor de Rechten van de Mens (FIRM) liet nog niets van zich horen: kennelijk is een dossier niet belangrijk genoeg wanneer het om financiële gegevens gaat.

Het gebrek aan debat verraadt niet eens kwade wil, maar getuigt vooral van politieke luiheid. De maatregel lijkt onschuldig omdat het slechts over gegevens gaat. Data geven echter informatie over gedrag, en wie gedrag systematisch screent, Controleert mensen. Wie mensen Controleert zonder aanleiding, overschrijdt de grens van de vrije rechtsstaat.

De minister hoopt dat deze maatregel zal passeren als een voetnoot. De spreker wil er daarentegen voor zorgen dat er een daadwerkelijk debat wordt gevoerd. Een wet houdende diverse bepalingen is bedoeld voor kleine aanpassingen en aanvullingen van technische leemtes. Indien de logica wordt aanvaard dat fundamentele bevoegdheidsuitbreidingen zonder grondig debat mogelijk zijn in een dergelijke tekst, dan verliest het Parlement elke substantiële betekenis en dient het enkel nog om een administratief fait accompli formeel te bekrachtigen.

De heer Van Quickenborne stelt geen verstrekkende eisen: hij is niet de bedoeling om de strijd tegen fraude op te geven of om technologie te wantrouwen. Zijn voornaamste vraag is dat de commissieleden begrijpen wat zij zullen legaliseren.

— Gebrekkige wetgeving

De voorliggende tekst is op sommige vlakken onduidelijk. Zo luidt een alinea in amendement nr. 16 (DOC 56 0963/005), waarmee een nieuw artikel 95/3 wordt ingevoerd, als volgt:

“De concrete gegevens afkomstig van het voornoemd Centraal aanspreekpunt die overeenkomstig het eerste lid verwerkt worden, mogen niet gecommuniceerd worden aan de ambtenaar bevoegd om de Controle uit te voeren, behalve indien aan de voorwaarden voorzien in artikel 322, WIB voldaan is.”

L'intervenant regrette que le gouvernement souhaite prendre exactement la même mesure dans le domaine financier en Belgique, mais sans aucune discussion, audition, aucun débat de société ou analyse. Si *chat control* avait été introduit de la même manière, à l'aide d'amendements retirés et redéposés, les protestations auraient été innombrables. Or, la mesure à l'examen au sein de cette commission passe sans grande publicité.

L'Institut fédéral des droits humains (IFDH), non plus, ne s'est pas encore manifesté. Apparemment, un dossier n'est pas jugé suffisamment important lorsqu'il concerne des données financières.

L'absence de débat trahit moins une mauvaise volonté qu'une paresse politique. La mesure paraît innocente car elle ne concerne que des données. Or, celles-ci fournissent une source d'informations sur nos comportements. Et ceux qui décortiquent systématiquement nos comportements contrôlent les individus. Et ceux qui contrôlent les individus sans motif valable outrepassent les limites de l'état de droit libre.

Le ministre espère que cette mesure passera comme une note de bas de page. L'intervenant souhaite, quant à lui, faire en sorte que l'on en débattenne réellement. Une loi portant des dispositions diverses a pour objet d'apporter des modifications et des ajouts mineurs afin de combler des lacunes techniques. Si l'on accepte le principe selon lequel des compétences peuvent être fondamentalement élargies dans ce genre de texte sans débat approfondi, le Parlement perdra toute signification substantielle et ne servira plus qu'à valider formellement un fait accompli administratif.

M. Van Quickenborne ne pose pas d'exigences radicales. Son intention n'est pas d'abandonner la lutte contre la fraude ou de se méfier de la technologie. Sa principale demande est que les membres de la commission comprennent ce qu'ils s'approprient à légaliser.

— Une législation lacunaire

Le texte à l'examen manque de clarté à certains égards. Par exemple, un alinéa de l'amendement n° 16 (DOC 56 0963/005), qui introduit un nouvel article 95/3, est rédigé comme suit:

“Les données concrètes provenant du Point de contact central précité qui sont traitées conformément à l'alinéa 1^{er}, ne peuvent pas être communiquées au fonctionnaire compétent pour effectuer le contrôle, sauf si les conditions prévues dans l'article 322, CIR 92 sont remplies.”

Het getrapte systeem van artikel 322 WIB 92 bepaalt voorsnóg dat de bevoegde diensten eerst een vraag om inlichtingen aan de belastingplichtigen moeten stellen en dat er aanwijzingen van belastingontduiking moeten zijn. Indien de betrokkene binnen de maand niet antwoordt, dan is de raadpleging van het CAP geoorloofd.

Het merkwaardige is dat de ambtenaar die een vraag om inlichtingen aan de belastingplichtige moet stellen, niet zal weten waarom hij een bepaald dossier krijgt toegewezen, aangezien deze informatie geheim is. Wat moet hij dan vragen aan de betrokkene? Volgens fiscale experts wil men met deze bepaling in amendement nr. 16 vermijden dat er dubbel werk zou moeten gebeuren: wanneer een dossier opgemaakt is naar aanleiding van fiscale fraude, dan hoeft niet opnieuw het getrapte systeem gevolgd te worden, maar kan men de gegevens rechtstreeks raadplegen. Dat is in de ogen van de heer Van Quickenborne een eigenaardige uitleg, omdat de tekst zich beperkt tot artikel 322 van het WIB, en niets zegt over bijvoorbeeld btw of andere wetboeken waar een dergelijk systeem ook geldt.

De minister gaf aan dat enkel een ambtenaar met de titel van adviseur de dossiers in kwestie zal mogen behandelen. In de verantwoording bij amendement nr. 16 staat inderdaad: “Alleen een ambtenaar met de titel van ten minste adviseur kan besluiten om een dossier in het werkplan op te nemen”. Dit staat echter niet in de tekst zelf. Hoe komt het dan dat in artikel 322 WIB 92, een basisartikel in de fiscaliteit, wel systematisch wordt verwezen naar titels van bepaalde ambtenaren? Betreft het een vergetelheid of gaat het om politieke luiheid?

Er lijkt zelfs geen interkabinettenwerkgroep over deze tekst te hebben vergaderd. Het doet de vraag rijzen of de tekst rechtstreeks van een kernkabinet komt. De heer Niels Tas (Vooruit) gaf zelf reeds aan dat deze bepaling door zijn partij reeds tijdens de Vivaldi-regering zonder succes naar voor werd geschoven. Deze keer raakte de maatregel wel voorbij de Ministerraad.

Volgens de minister wordt de ernstige georganiseerde fraude gevisieerd. In de tekst is echter ook sprake van “indiciaire tekorten”. Dit betekent dat de belastingambtenaar uitgaven vaststelt die niet met iemands inkomsten verantwoord kunnen worden. Er kan in dat geval een belasting op die uitgaven geheven worden. Dergelijke indiciaire tekorten komen echter allermínst altijd overeen met ernstige georganiseerde fraude. Toch wordt in de verantwoording als voorbeeld verwezen naar fraude, terwijl in de wettekst zelf sprake is van “risico tot het plegen van een inbreuk op een wet of een reglementering”. Beantwoordt een verkeersovertreding of een

La procédure par paliers de l'article 322 du CIR 92 prévoit actuellement que les services compétents doivent d'abord adresser une demande de renseignements au contribuable et qu'il doit exister des indices de fraude fiscale. Si l'intéressé ne répond pas dans un délai d'un mois, la consultation du PCC est alors autorisée.

Ce qui semble curieux, c'est que le fonctionnaire chargé d'adresser une demande de renseignements au contribuable ignorera pourquoi un dossier particulier lui a été attribué, cette information étant confidentielle. Que doit-il, dès lors, demander à l'intéressé? Selon certains experts fiscaux, la disposition contenue dans l'amendement n° 16 viserait à éviter de faire deux fois le même travail: lorsqu'un dossier est constitué à la suite d'une fraude fiscale, il n'est plus nécessaire de recourir à nouveau au système par paliers: les données peuvent être consultées directement. M. Van Quickenborne estime que cette interprétation est étrange, car le texte se limite à l'article 322 du CIR et ne fait aucune référence, par exemple, à la législation sur la TVA ni à d'autres codes où un système similaire s'applique également.

Le ministre a indiqué que seuls les fonctionnaires portant le titre de conseiller seraient autorisés à traiter les dossiers concernés. Dans la justification de l'amendement n° 16, on peut en effet lire: “Seul un fonctionnaire du titre de conseiller au moins peut décider d'inscrire un dossier au plan de travail”. Toutefois, cette précision ne figure pas dans le texte lui-même. Comment se fait-il alors que l'article 322 du CIR 92, un article fondamental en matière fiscale, fasse systématiquement référence aux titres de certains fonctionnaires? S'agit-il d'un oubli ou d'une paresse politique?

Il semble même qu'aucun groupe de travail interkabinet ne se soit réuni au sujet de ce texte. Cela soulève la question de savoir s'il provient directement du cabinet restreint. M. Niels Tas (Vooruit) a d'ailleurs indiqué que son parti avait déjà proposé cette disposition, sans succès, sous le gouvernement Vivaldi. Cette fois-ci, la mesure a toutefois franchi l'étape du Conseil des ministres.

Selon le ministre, la mesure vise la fraude grave et organisée. Cependant, le texte mentionne également des “déficits indiciaires”, c'est-à-dire les dépenses constatées par le fisc qui ne peuvent être justifiées par les revenus d'une personne. Un impôt peut alors être prélevé sur ces dépenses. Or, ces déficits indiciaires ne correspondent pas toujours à une fraude grave et organisée, loin s'en faut. Pourtant, dans la justification, la fraude est citée comme exemple, alors que le texte de loi parle de “risque de commission d'une infraction à une loi ou à une réglementation”. Une infraction routière ou une amende SAC relèveraient-elles également de

GAS-boete daar dan ook aan? De tekst lijkt met haken en ogen aan elkaar te hangen.

De heer Van Quickenborne benadrukt dat een breed parlementair debat geen luxe is, maar een plicht. Hoorzittingen zouden zeer zinvol zijn, en niet pas na het stemmen van het voorliggende wetsontwerp, zoals de meerderheid voorstelt. Dit zou meer klaarheid kunnen scheppen over de manier waarop datamining precies in zijn werk gaat of over wat er precies in de Data & Access Management (DAM)-fiches staat. De GBA en het CAP zouden eveneens gehoord moeten worden, om te weten te komen of de betrokken instanties voorbereid zijn. Zo zijn de DAM-fiches één van de pijlers waarop het hele systeem gebaseerd zal worden, maar weet de fiscale administratie zelf niet eens hoe dit precies in zijn werk gaat.

Een volgend punt van kritiek is de inwerkingtreding van de voorliggende maatregelen. Volgens insiders zijn er geen voorbereidingen getroffen om het systeem te laten functioneren, terwijl de wetgeving reeds tien dagen na publicatie in het *Belgisch Staatsblad* van kracht wordt.

Bij de Nationale Bank van België (NBB), die het CAP beheert, weet men zelfs niet hoe de gegevensoverdracht precies zal verlopen. Er zou zelfs nog geen vergadering over deze uitwisseling hebben plaatsgevonden, wat volgens de spreker van amateurisme getuigt.

Bepalingen inzake uitvoeringsbesluiten ontbreken eveneens in het voornoemde amendement nr. 16 (DOC 56 0963/005). Is de voorliggende tekst dan zo volledig dat er geen enkele modaliteit door middel van een koninklijk of ministerieel besluit zal moeten worden geregeld? Het is slechts één van de vele redenen om het debat grondiger te voeren.

— Structurele gelijkenissen met chat control

De heer Van Quickenborne gaat vervolgens verder in op de parallellen met *chat control*. Het voorstel van de Europese Commissie kwam neer op preventie via geautomatiseerde detectie, in tegenstelling tot enkel repressie na een klacht. Het meest controversiële element hield in dat apps hun end-to-end-versleuteling moesten doorbreken om berichten te kunnen scannen, of lokale algoritmes moesten inzetten die elke boodschap op een toestel controleren voor verzending. Waar de overheid vroeger enkel toegang kreeg tot berichten na een rechterlijk bevel, zou nu elk gesprek potentieel kunnen worden gescand. Privacy-experten gewagen van een

cette catégorie? Le texte paraît pour le moins confus et mal structuré.

M. Van Quickenborne souligne qu'un large débat parlementaire n'est pas un luxe, mais un devoir. Il serait très utile d'organiser des auditions, et pas seulement après le vote du projet de loi à l'examen, comme le propose la majorité. Cela permettrait de clarifier davantage les modalités de fonctionnement du *data mining* ou le contenu exact des fiches *Data & Access Management* (DAM). L'APD et le PCC devraient également être entendus afin de vérifier si les instances concernées y sont préparées. En effet, les fiches DAM constituent l'un des piliers sur lesquels reposera l'ensemble du système, mais l'administration fiscale elle-même ignore encore comment tout cela fonctionnera concrètement.

Un autre élément de critique concerne l'entrée en vigueur des mesures proposées. Selon certaines personnes bien informées, aucune préparation n'a été effectuée pour permettre le fonctionnement du système, alors que la législation entrera en vigueur dès dix jours après sa publication au *Moniteur belge*.

La Banque nationale de Belgique (BNB), chargée de gérer le PCC, ignore toujours comment se déroulera au juste le transfert des données. Aucune réunion n'aurait encore eu lieu à ce sujet, ce qui, selon l'intervenant, révèle un manque de professionnalisme.

Les dispositions relatives aux arrêtés d'exécution font également défaut dans l'amendement n° 16 précité (DOC 56 0963/005). Le texte à l'examen est-il donc si exhaustif qu'aucune modalité ne devra être fixée par arrêté royal ou ministériel? Voilà une des nombreuses raisons pour lesquelles le débat doit être approfondi.

— Similarités structurelles avec chat control

M. Van Quickenborne épingle ensuite d'autres similarités avec *chat control*. La proposition de la Commission européenne revenait à faire de la prévention au moyen de la détection automatisée, au lieu de ne faire que de la répression à la suite d'une plainte. L'élément le plus controversé de ce dispositif était que les applications numériques devaient briser leur chiffrement de bout en bout pour pouvoir scanner les messages, ou recourir à des algorithmes locaux capables de contrôler chaque message sur un appareil avant envoi. Là où les pouvoirs publics ne pouvaient auparavant accéder à des messages qu'en vertu d'une injonction judiciaire, ce

digitaal sleepnet: een systeem dat niet op verdenking is gebaseerd, maar op een mogelijke kans op afwijking.

De gelijkenis met het controleren van financiële communicatie, zoals in dit wetsontwerp voorligt, is zeer sterk. De doelstelling – bij *chat control* de preventie van strafbare inhoud – loopt gelijk met het doel van de minister, namelijk de preventie van fiscale fraude. De werking is eveneens vergelijkbaar: algoritmes scannen bij *chat control* elk bericht en screenen bij “*money control*” elke bankrekening. De aard van toezicht is in beide gevallen preventief, massaal en niet gebaseerd op verdenking. Het risico in beide systemen is het doorbreken van de vertrouwelijkheid, hetzij van communicatie, hetzij van financiële handelingen.

Het kernprobleem is telkens dat gericht opsporen wordt vervangen door constant scannen en analyseren. Bij *chat control* wordt iedereen potentieel aanzien als pleger van kindermisbruik; bij *money control* wordt elke burger potentieel een fraudeur. De gelijkenissen zijn frappant.

Beide systemen vertrekken van een technologische logica: als alles wordt gescand, raakt misbruik sneller opgespoord. Het is echter niet omdat de mogelijkheid technologisch bestaat, dat het ook geoorloofd is. De twee mechanismen botsen op dezelfde juridische grens: een democratische rechtsstaat mag niet massaal preventief onderzoeken zonder aanleiding.

— Juridische parallellen met *chat control*

Een juridische parallel is dat beide systemen het legaliteitsbeginsel dreigen uit te hollen. Er is geen duidelijk omschreven aanleiding voor een onderzoek, enkel een algoritmische trigger. Een overheid handelt niet meer op basis van feiten, maar op basis van vermoedens die ze zelf genereert.

Een volgende juridische parallel berust op artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM): het Europees Hof voor de Rechten van de Mens (EHRM) heeft herhaaldelijk geoordeeld dat algemene ongedifferentieerde surveillance, ook met een legitiem doel, in strijd is met artikel 8 van het Verdrag. In dat verband kan verwezen worden naar het arrest *Big Brother Watch v. UK* van het EHRM van 2021, alsook

dispositif leur aurait potentiellement permis de scanner chaque discussion. Les experts du respect de la vie privée ont parlé de contrôle numérique généralisé: un système reposant non pas sur l’existence de soupçons, mais sur un risque d’infraction.

Les similarités avec le contrôle des communications financières prévu dans le projet de loi à l’examen sont très fortes. L’objectif de *chat control* (la prévention des contenus illicites) est comparable à celui du ministre (la prévention de la fraude fiscale). Le fonctionnement des deux dispositifs est également comparable: les algorithmes de *chat control* scanneraient chaque message, tandis que ceux de *money control* scanneraient chaque compte bancaire. Dans les deux cas, la nature de la surveillance serait préventive, généralisée et ne reposerait pas sur l’existence de soupçons. Ces deux dispositifs impliquent un risque de rupture de la confidentialité, soit de la communication, soit des opérations financières.

Le problème majeur des deux dispositifs est qu’ils prévoient de remplacer la détection ciblée par un recours constant à des opérations de scannage et d’analyse. Dans le cadre de *chat control*, chacun utilisateur serait considéré comme un auteur potentiel d’abus sexuels sur enfants, alors que, dans le cadre de *money control*, chaque citoyen serait considéré comme un fraudeur potentiel. Les similarités sont frappantes.

Les deux dispositifs reposent sur une logique technologique: un scannage généralisé permettrait de détecter plus rapidement les abus. Cependant, ce n’est pas parce que la technologie permet de le faire que cela doit être autorisé. Ces deux dispositifs se heurtent à la même barrière juridique: un État de droit démocratique ne peut pas procéder à des investigations préventives massives sans motif.

— Parallèles juridiques avec *chat control*

L’intervenant établit un parallèle juridique entre ces deux dispositifs: ils risquent de saper le principe de légalité. En effet, ils ne prévoient aucun motif clair pour l’ouverture d’une enquête, mais uniquement un déclencheur algorithmique. En conséquence, les pouvoirs publics n’agiront plus sur la base de faits, mais seulement sur la base de soupçons qu’ils ont eux-mêmes générés.

L’intervenant établit un autre parallèle juridique, en lien avec l’article 8 de la Convention européenne des droits de l’homme (CEDH): la Cour européenne des droits de l’homme (CEDH) a jugé à plusieurs reprises qu’une surveillance généralisée et indifférenciée était contraire à l’article 8 de ladite Convention, même lorsque celle-ci poursuivait un objectif légitime. À cet égard, il peut être renvoyé à l’arrêt *Big Brother Watch c. Royaume-Uni*

naar de SyRi-wetgeving die leidde tot de Nederlandse toeslagenaffaire.

Een derde juridische parallel is artikel 22 van de Grondwet waarmee niet enkel communicatie, maar ook financiële privacy wordt beschermd. De CAP-wet van 8 juli 2018 was en is grondwettelijk enkel verdedigbaar omdat ze gerichte, beperkte toegang tot de databank voorzag.

De spreker verwijst in dit verband naar arrest nr. 162/2022 van het Grondwettelijk Hof. De belangenvereniging “The Ministry of Privacy” trok ten strijde tegen de programmawet van 20 december 2020 die een aanpassing doorvoerde in de wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van rekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest. Het Grondwettelijk Hof heeft deze CAP-wet uiteindelijk in stand gehouden met als belangrijkste motivatie dat het CAP enkel kan worden geconsulteerd in heel specifieke gevallen, zijnde bij aanwijzingen van fraude en de niet-bereidwilligheid van belastingplichtigen om mee te werken. Datamining ondergraaft echter precies dat fundament.

— Een verontrustende evolutie

De evolutie naar aanleiding van *chat control* en *money control* is gevaarlijk.

Vooreerst gaat het om mechanismen die in stappen werken. Eerst begint men over iedereen gegevens te verzamelen, dan volgt detectie, algoritmen zoeken patronen van afwijking en vervolgens gaat men over tot profilering. Resultaten worden gebruikt om risico's toe te wijzen. Het klinkt neutraal, maar het betekent een fundamentele omkering van het vermoeden van onschuld.

Een burger wordt niet gecontroleerd omdat er iets gebeurd is, maar omdat het systeem denkt dat hij zou kunnen afwijken. Beide mechanismen zijn symptomen van dezelfde bestuurslogica: de staat beperkt zich niet langer tot het opsporen van misbruik, maar stelt zich structureel in op de mogelijkheid van afwijking bij iedereen.

Dit gaat gepaard met maatschappelijke bijwerkingen: zelfcensuur (mensen spreken en handelen anders als ze weten dat hun woorden of centen kunnen worden gecontroleerd), verlies van vertrouwen (de burger gaat de overheid zien als een permanente controleur in plaats

rendu en 2021 par la CEDH, ainsi qu'à la législation néerlandaise SyRi, qui a débouché sur le scandale des allocations familiales dans ce pays.

Un troisième parallèle juridique épinglé par l'intervenant concerne l'article 22 de la Constitution, qui protège non seulement la correspondance, mais aussi la vie privée financière. L'intervenant souligne que la loi du 8 juillet 2018 relative au PCC n'était et n'est défendable sur le plan constitutionnel que parce qu'elle prévoit un accès ciblé et restreint à cette base de données.

À cet égard, le membre renvoie à l'arrêt n° 162/2022 rendu par la Cour constitutionnelle dans le cadre du recours introduit par le groupement d'intérêts *The Ministry of Privacy* contre la loi-programme du 20 décembre 2020, qui modifiait la loi du 8 juillet 2018 portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt. La Cour constitutionnelle a finalement décidé de ne pas annuler la loi relative au PCC, principalement parce que les consultations du PCC ne peuvent avoir lieu que dans des cas très spécifiques, à savoir lorsqu'il existe des indications de fraude et lorsque des contribuables refusent de coopérer. Or, l'exploration de données sape justement cette condition fondamentale.

— Une évolution inquiétante

L'évolution induite par *chat control* et *money control* est dangereuse.

Premièrement, il s'agit de mécanismes qui fonctionnent par étapes: la première consiste à collecter des données sur tout le monde, la deuxième à détecter des anomalies à l'aide d'algorithmes et la troisième à faire du profilage. Les résultats sont ensuite utilisés pour attribuer des degrés de risque. Ce qui peut sembler neutre constitue en réalité un renversement fondamental du principe de la présomption d'innocence.

En effet, un citoyen ne sera plus contrôlé en raison d'un événement qui est survenu, mais parce que le système pense qu'il pourrait commettre une infraction. Ces deux mécanismes sont symptomatiques de la même logique administrative: l'État ne se borne plus à détecter les abus commis, mais part du principe que chaque citoyen pourrait en commettre.

Deuxièmement, cette tendance produira des effets secondaires dans la société: l'autocensure (les personnes parlent et agissent différemment lorsqu'elles savent que leurs paroles ou leurs opérations financières peuvent être contrôlées), la perte de confiance (le citoyen verra

van als beschermheer) en de normalisering van intrusieve technologie. Zodra datamining is ingevoerd, wordt het zeer moeilijk om terug te keren naar een niet-geobserveerde samenleving. De democratische reflex, waarbij het aanwenden van macht de nodige verantwoording vereist, wordt vervangen door een technologisch reflex.

De spreker verwacht dan ook dat de minister haarfijn uitlegt waarom hij zich tegen *chat control* heeft gekant, maar wel de voorliggende maatregel wil doorvoeren. Het zijn twee gezichten van dezelfde medaille. Kan de minister de commissie ervan overtuigen dat het twee verschillende zaken zijn?

De democratie hoeft niet blind te zijn om vrij te blijven, maar ze moet leren kijken met grenzen. De lijn tussen bescherming en beheersing vervaagt met de genoemde mechanismen. In beide gevallen is de oplossing dezelfde: wettelijke precisie (alle essentiële elementen opnemen in de wet, zoals de Raad van State opmerkt), onafhankelijke toetsing en de erkenning dat niet alles weten soms de hoogste vorm van vertrouwen is.

— De facto invoering van een vermogenskadaster

Er is meer aan de hand: *money control* is niet alleen de *chat control* van de financiële wereld, het is ook de poort naar een vermogenskadaster, een socialistische wensdroom. In *Het Nieuwsblad* van 1 oktober 2025 staat dat Vooruit geen nieuw vermogenskadaster wil aanleggen, maar wel mikt op het openstellen van het CAP voor de fiscus. Daar zit de informatie over het financiële vermogen van alle Belgen sowieso al gebundeld.

Dankzij de voorliggende wetgeving zullen deze gegevens inderdaad voor het grijpen liggen, aangezien er geen indicatie van fraude noch bereidwilligheid van de belastingplichtigen meer hoeft te zijn alvorens de databank in te kijken.

Op een vraag van de heer Kjell Vander Elst (Open Vld) antwoordde de minister dat er geen sprake kan zijn van een vermogenskadaster. Toch bedient hij Vooruit op zijn wenken en zet hij deze deur open door middel van toegang tot het CAP. Wat zijn de beloften van de minister waard als hij een mechanisme invoert dat een systematische analyse van financiële data toelaat, zonder voorafgaand vermoeden?

Het CAP bevat de gegevens van alle bankrekeningen. Vandaag mag het enkel geraadpleegd worden bij een aangetoond vermoeden van fraude, wat ervoor zorgt

l'État comme un contrôleur permanent au lieu d'un protecteur) et la normalisation des technologies intrusives. Dès que l'exploration de données aura été instaurée, il sera extrêmement difficile de revenir à une société sans surveillance. Le réflexe démocratique, qui implique de motiver toute décision, sera remplacé par un réflexe technologique.

L'intervenant attend donc du ministre qu'il explique en détail pourquoi il souhaite instaurer la mesure à l'examen alors qu'il s'est opposé à *chat control*. En effet, ce sont les deux faces d'une même pièce. Le ministre serait-il en mesure de convaincre la commission qu'il s'agit en réalité de deux choses différentes?

La démocratie ne doit pas forcément être aveugle pour rester libérale, mais elle doit apprendre à composer avec certaines limites. Les mécanismes précités estomperont la frontière entre la protection et le contrôle. Dans les deux cas, les solutions à apporter sont identiques: l'apport de précisions juridiques (inscription de tous les éléments essentiels dans la loi, comme l'a souligné le Conseil d'État), un contrôle indépendant et la reconnaissance que ne pas tout savoir est parfois la forme de confiance la plus grande.

— Introduction concrète d'un cadastre du patrimoine

Les enjeux sont plus larges: le *money control* n'est pas seulement le *chat control* du monde financier, mais c'est également l'amorce du cadastre du patrimoine que les socialistes appellent de leurs vœux. Selon l'édition du *Nieuwsblad* du 1^{er} octobre 2025, le parti Vooruit ne souhaite pas créer un nouveau cadastre du patrimoine, mais entend permettre au fisc d'accéder au PCC, qui rassemble déjà les informations sur le patrimoine financier de tous les Belges.

La législation à l'examen ouvrira effectivement l'accès à ces données, puisqu'il ne sera plus nécessaire de disposer d'un indice de fraude ou de s'appuyer sur la bonne volonté des contribuables pour pouvoir consulter la banque de données.

En réponse à une question de M. Kjell Vander Elst (Open Vld), le ministre a indiqué qu'il n'était pas question d'établir un cadastre du patrimoine. Or, il répond aux attentes de Vooruit et ouvre la voie à ce cadastre en ouvrant l'accès au PCC. Que valent les promesses du ministre s'il met en place un mécanisme qui permettra d'analyser systématiquement les données financières en l'absence de présomption préalable?

Le PCC contient les données de tous les comptes bancaires. Aujourd'hui, il ne peut être consulté qu'en cas de suspicion avérée de fraude, ce qui permet à la banque

dat de databank de grondwettelijke toets doorstaat. Deze constitutionele *firewall* wordt door de minister echter neergehaald: niet langer een vermoeden leidt tot raadpleging, maar raadpleging leidt tot een vermoeden. Het advies van de GBA zegt dat deze logica het fundamentele beginsel van doelbinding ondermijnt en de proportionaliteit schendt.

Zodra *money control* bestaat en operationeel is, is het vermogenskadaster een feit. Sommige fracties zijn er niet rouwig om dat deze maatregel aan het tot nog toe povere palmares van deze regering wordt toegevoegd.

Een vermogenskadaster maakt financiële gegevens permanent beschikbaar voor de overheid. Het beantwoordt aan drie criteria: volledigheid (het dekt alle burgers, ongeacht verdenking, en alle rekeningen, saldi en financiële contracten), actualiteit (de gegevens worden systematisch bijgewerkt, de saldi twee keer per jaar) en toegankelijkheid (overheidsdiensten kunnen er rechtstreeks in raadplegen of zoeken). Dit zijn precies de criteria waaraan "*money control*" beantwoordt. Het is de reden waarom de Raad van State impliciet stelde dat de uitbreiding van de CAP-doeleinden de facto zou neerkomen op de creatie van een vermogenskadaster, zonder wettelijke basis. Dat is een fundamenteel probleem.

Het komt neer op functievermenging: zodra de fiscus structureel toegang krijgt tot het CAP, sluipt het vermogenskadaster immers binnen in het dagelijks bestuur.

De regeringsamendementen bevatten tevens een bepaling die de fiscus de toelating geeft om effectenrekeningen in te kijken zonder vermoeden van fraude, in tegenstelling tot bankrekeningen, waar dat vermoeden wel moet bestaan. Het probleem is dat de fiscus krachtens verschillende artikelen in het Wetboek van de Inkomstenbelastingen niet alleen gerechtigd, maar zelfs verplicht is om op een legitieme manier verkregen informatie te delen met andere fiscale instanties. Indien men bijvoorbeeld een effectenrekening kan inkijken, dan kan die informatie ook gebruikt worden om na te gaan of de meerwaardebelasting wel correct werd toegepast en of men zich in andere fiscale wetgeving correct heeft gedragen. Het CAP wordt met andere woorden een databank die openstaat voor systematische screening. Dit is zeer beangstigend. De vraag is niet of het vermogenskadaster bestaat, maar waarvoor het zal worden gebruikt.

de données de résister au contrôle constitutionnel. Le ministre abat toutefois ce rempart constitutionnel: ce ne sont plus les soupçons qui entraîneront la consultation, mais ce sera la consultation qui fera naître les soupçons. Selon l'avis de l'APD, cette logique porte atteinte au principe fondamental de limitation des finalités et viole le principe de proportionnalité.

Dès que le *money control* sera en place et opérationnel, le cadastre du patrimoine existera. Certains groupes politiques ne regrettent pas que cette mesure vienne s'ajouter au bilan jusqu'à présent médiocre du gouvernement actuel.

Ce cadastre du patrimoine permettra aux autorités publiques d'accéder en tout temps aux données financières. Il répond à trois critères: au critère de l'exhaustivité (il vise tous les citoyens, indépendamment de tout soupçon, et l'ensemble des comptes, des soldes et des contrats financiers), au critère de l'actualité (les données seront systématiquement mises à jour, et les soldes le seront deux fois par an) et au critère de l'accessibilité (les services publics pourront directement le consulter ou y effectuer des recherches). Il s'agit précisément des critères du "*money control*" et c'est pourquoi le Conseil d'État a implicitement indiqué que l'élargissement des objectifs du PCC reviendrait de facto à créer un cadastre du patrimoine en l'absence de toute base légale. Il s'agit d'un problème fondamental.

Cela revient à confondre les fonctions: dès que le fisc aura structurellement accès au PCC, le cadastre du patrimoine deviendra effectivement réalité dans la gestion journalière.

Les amendements du gouvernement contiennent également une disposition visant à autoriser l'administration fiscale à consulter les comptes-titres en l'absence de soupçon de fraude, contrairement à ce qui est prévu pour les comptes bancaires, pour lesquels ce soupçon doit exister. Or, le problème est qu'en vertu de plusieurs articles du Code des impôts sur les revenus, l'administration fiscale est non seulement autorisée à partager les informations obtenues de manière légitime avec d'autres autorités fiscales, mais également tenue de le faire. Par exemple, la consultation d'un compte-titres permettra également d'utiliser les informations recueillies pour vérifier si la taxe sur les plus-values a été correctement appliquée et si d'autres dispositions fiscales ont été respectées. En d'autres termes, le PCC deviendra une banque de données qui pourra servir à un contrôle systématique, ce qui est très inquiétant. La question n'est pas de savoir si le cadastre du patrimoine existera, mais à quoi il servira.

Het is behoorlijk ironisch dat de partij die altijd waar-schuwde voor een dergelijk vermogenskadaster het nu zelf uitbouwt. Volgens allerhande stoere verklaringen zou dit nooit ofte nimmer passeren, maar ondertussen wordt software ingevoerd die een identiek instrument technisch mogelijk maakt via het CAP.

Andere landen hebben de les al geleerd. In Nederland leidde het SyRI-project tot veroordeling wegens schending van artikel 8 EVRM (Rechtbank Den Haag, 5 februari 2020). In Frankrijk werd de fiscale datamining beperkt tot concrete fraudezaken, met jaarlijkse rapportering aan de CNIL. In Duitsland werd het ELENA-project stopgezet omdat het vertrouwen van burgers te zwaar beschadigd was. België lijkt nu de omgekeerde richting te nemen. Wat elders werd afgebouwd, wordt hier opgebouwd – en dat zonder wet, enkel met uitvoeringsbesluiten en platformkoppelingen.

Een digitale overheid is niet automatisch een transparante overheid. Transparantie vereist controle op de controleur. Maar *money control* bevat geen audit-mechanisme voor burgers, enkel voor de fiscus zelf. De logboeken zijn niet toegankelijk, de algoritmen niet uitlegbaar, de foutenmarge onbekend. De burger krijgt geen kennisgeving wanneer zijn gegevens worden geanalyseerd. Er is dus geen reëel rechtsmiddel tegen een fout signaal. Dat is de essentie van het probleem: machtsconcentratie zonder tegenmacht.

De ironie is dat het CAP, als men het correct gebruikt, een nuttig instrument is. Gerichte raadpleging bij vermoeden is efficiënt, wettig en proportioneel. Maar structurele koppeling met *money control* creëert een permanent financieel panopticum – een spiegelpaleis waar iedereen gezien wordt, maar niemand nog weet door wie.

Financiële privacy is geen luxeproduct. Ze vormt een deel van de persoonlijke waardigheid. Wie weet dat elke overschrijving kan worden bekeken, verandert onbewust zijn gedrag. Dat heet in de sociologie het *chilling effect*: het zelfcensureren uit angst om in een profiel te passen. In zo'n samenleving is de burger niet meer vrij, maar voorzichtig. En een samenleving van voorzichtige burgers is geen vrije samenleving.

Voorstanders zullen zeggen: “maar we doen dit enkel om fraude te bestrijden.” Maar dat argument faalt zodra

Il est assez ironique que le parti qui a toujours mis en garde contre ce cadastre œuvre aujourd'hui à sa mise en place. Alors que, selon de nombreuses déclarations tonitruantes, ce cadastre ne devait jamais voir le jour, on assiste aujourd'hui à l'arrivée d'un logiciel qui permettra techniquement de créer un instrument identique en passant par le PCC.

D'autres pays ont déjà tiré les enseignements de cette expérience. Aux Pays-Bas, le projet SyRI a donné lieu à une condamnation pour violation de l'article 8 de la CEDH (Tribunal de La Haye, 5 février 2020). En France, l'exploration des données fiscales a été limitée aux cas concrets de fraude, et assortie de l'obligation de faire annuellement rapport à la CNIL. L'Allemagne a mis fin au projet ELENA parce qu'il avait trop sérieusement entamé la confiance des citoyens. La Belgique semble s'engager aujourd'hui dans la direction opposée. Elle entend adopter des mesures abrogées ailleurs, sans passer par la voie légale et seulement au travers d'arrêtés d'exécution et d'interconnexions entre plusieurs plateformes.

Les autorités publiques numérisées ne sont pas toujours transparentes. La transparence impose de contrôler le contrôleur. Or, le *money control* ne prévoit aucun mécanisme d'audit pour les citoyens. Il ne prévoit ce mécanisme que pour l'administration fiscale. Les journaux de connexion ne seront pas accessibles, les algorithmes échapperont à toute explication, et la marge d'erreur est inconnue. Les citoyens ne recevront aucune notification lorsque leurs données seront analysées. Aucun recours réel n'a donc été prévu contre ce signal erroné. C'est là que le bât blesse, c'est-à-dire dans une concentration du pouvoir dépourvue de tout contre-pouvoir.

L'ironie, c'est que le PCC, est un instrument utile lorsqu'il est utilisé à bon escient. La consultation ciblée en cas de présomption est en effet efficace, légale et proportionnée. Par contre, son association structurelle au *money control* reviendra à mettre en place un panoptique financier permanent, un palais des glaces où tout le monde sera observé, mais sans plus savoir par qui.

Le respect de la vie privée financière n'est pas un luxe, mais relève de la dignité personnelle. S'ils savent que chaque virement bancaire pourra être consulté, les citoyens changeront inconsciemment de comportement. En sociologie, ce phénomène s'appelle l'effet dissuasif (*chilling effect*). Il s'agit de l'autocensure causée par la crainte d'être profilé. Dans les sociétés de ce type, les citoyens ne sont plus libres, mais prudents, et une société de citoyens prudents n'est pas une société libre.

Les partisans de cet outil diront qu'il servira seulement à lutter contre la fraude. Or, cet argument n'est

men alle burgers screent om enkele fraudeurs te vinden. Fraude opsporen mag nooit een alibi worden voor massale dataverwerking. De efficiëntie is bovendien illusoir: hoe groter de dataset, hoe meer vals-positieven.

En elke fout kost mensen tijd, geld en reputatie.

De wetgever heeft twee keuzes: ofwel bevestigen dat *money control* enkel mag worden ingezet bij concreet vermoeden, met duidelijke wettelijke grenzen; ofwel erkennen dat men een vermogenskadaster instelt en daar een nieuwe wet voor maakt, met parlementaire waarborgen en open debat.

De woorden van minister Jambon – “*no pasarán*” – klinken moedig. Maar zodra *money control* in werking treedt, zijn ze hol. Het is precies dat systeem dat “naar een vermogenskadaster ruikt”.

Men hoeft geen register van vermogens aan te leggen als men al een datamijn heeft waarin alle financiële sporen samenkomen. De toegang tot het CAP is het kadaster.

— *De ontbrekende adviezen (ECB, Inspectie van Financiën en NBB)*

Er zijn wetten die door hun inhoud aandacht trekken, en er zijn wetten die door hun stilte iets verraden. De hervorming van het Centraal Aanspreekpunt – de uitbreiding tot geautomatiseerde risicoanalyse – behoort tot die tweede categorie. En wat ontbreekt, zijn drie adviezen die er volgens logica, gewoonte en soms zelfs verplichting hadden moeten zijn:

- het advies van de Europese Centrale Bank (ECB);
- het advies van de Inspectie van Financiën;
- het advies van de Nationale Bank van België (NBB).

Drie instellingen die niet alleen bevoegd, maar ook bekwaam zijn om te waarschuwen voor de financiële, budgettaire en privacyrisico's van een maatregel die bankgegevens structureel openstelt voor administratieve analyse.

Wie macht uitoefent over gegevens, moet eerst macht verdragen van toezicht. En dat toezicht begint met advies.

pas pertinent lorsque tous les citoyens sont contrôlés afin d'identifier quelques fraudeurs. La recherche de la fraude ne pourra jamais servir à cautionner le traitement massif des données. L'efficacité de ce système est en outre illusoire: plus l'ensemble de données est grand, plus le nombre de faux positifs augmente.

Qui plus est, chaque erreur aura un coût: perte de temps, perte d'argent ou atteinte à la réputation.

Deux options s'offrent au législateur: confirmer que le *money control* ne pourra être appliqué qu'en cas de soupçon concret, et l'assortir alors de limites légales claires, ou reconnaître qu'un cadastre du patrimoine sera mis en place et élaborer, à cet effet, une nouvelle loi assortie de garanties parlementaires et après un débat ouvert.

Si les mots “*no pasarán*” du ministre Jambon semblent courageux, l'entrée en vigueur du *money control* les videra de leur substance. C'est précisément ce système qui ressemble à un cadastre du patrimoine.

La création d'un cadastre du patrimoine sera superflue si l'on dispose d'une mine de données regroupant toutes les traces financières. Ouvrir l'accès au PCC équivaut à établir un cadastre.

— *Avis manquants (BCE, Inspection des finances et BNB)*

Certaines lois attirent l'attention par leur contenu, d'autres se rendent coupables de trahison par leur silence. La réforme du Point de contact central – son extension à l'analyse automatisée des risques – appartient à cette seconde catégorie. Ce silence est matérialisé en l'espèce par l'absence de trois avis qui, selon la logique, selon l'usage, voire selon une obligation légale, auraient dû être recueillis dans le cadre du projet de loi à l'examen:

- l'avis de la Banque centrale européenne (BCE);
- l'avis de l'Inspection des finances;
- l'avis de la Banque nationale de Belgique (BNB).

Ces trois institutions sont non seulement compétentes en la matière, mais elles sont aussi habilitées à mettre en garde contre les risques financiers, budgétaires et relatifs au respect de la vie privée qui découleraient d'une mesure visant à divulguer structurellement des données bancaires en vue d'une analyse administrative.

Toute autorité qui exerce un pouvoir sur des données doit d'abord accepter d'être contrôlée. Et ce contrôle passe préalablement par des avis.

1. Het advies van de ECB: een Europese plicht, geen formaliteit

De Europese Centrale Bank is niet zomaar een instelling die zich enkel met monetaire politiek bezighoudt. Sinds het Verdrag van Maastricht en vooral het Protocol nr. 4 bij het VWEU heeft zij een expliciete taak in het raadplegen van nationale autoriteiten over ontwerpen die de stabiliteit, de werking of de integriteit van financiële instellingen kunnen beïnvloeden.

Artikel 127, lid 4, VWEU en Besluit 98/415/EG van de Raad verplichten lidstaten om de ECB te raadplegen over “ontwerpen van wettelijke bepalingen op het gebied van de taken van de ECB, met name regels die van invloed zijn op financiële instellingen en betalingssystemen.”

Daaronder vallen expliciet:

- maatregelen inzake het toezicht op kredietinstellingen;
- regels inzake de rapportering en gegevensverwerking van banken;
- en elk ontwerp dat de verplichtingen of de aansprakelijkheid van financiële instellingen kan wijzigen.

De uitbreiding van het CAP raakt precies dat terrein. Ze verplicht banken om gegevens structureel te laten analyseren, niet meer enkel passief op te slaan. De aard van de verplichting wijzigt: van “ter beschikking houden” naar “beschikbaar stellen voor verwerking”.

Dat is geen technische nuance; het is een wijziging van het juridische en operationele statuut van bankgegevens.

Volgens vaste ECB-praktijk zou zo'n maatregel zonder uitzondering aan de Bank moeten worden voorgelegd. In andere lidstaten – bijvoorbeeld Spanje, Duitsland, Oostenrijk – worden zelfs minder verregaande wijzigingen standaard voor advies doorgestuurd.

Niet als beleefdheidsformule, maar omdat de ECB toeziet op de delicate balans tussen gegevensuitwisseling en financiële stabiliteit.

In België is dat niet gebeurd. Er is geen spoor van raadpleging in de parlementaire stukken. Geen vermelding in de memorie van toelichting, geen annex, geen samenvatting van advies.

1. Avis de la BCE: une obligation européenne, pas une formalité

La Banque centrale européenne n'est pas seulement une institution chargée de la politique monétaire. Depuis l'entrée en vigueur du traité de Maastricht et surtout du protocole n° 4 annexé au TFUE, elle a pour mission explicite de consulter les autorités nationales sur les projets pouvant affecter la stabilité, le fonctionnement ou l'intégrité des établissements financiers.

L'article 127, paragraphe 4, du TFUE et la décision 98/415/CE du Conseil imposent aux États membres de consulter la BCE sur tout projet de réglementation relevant de son domaine de compétence, et notamment en ce qui concerne les règles applicables aux établissements financiers et aux systèmes de paiement.

Sont visés explicitement:

- les mesures relatives au contrôle des établissements de crédit;
- les règles relatives au *reporting* et au traitement des données par les banques;
- et tout projet pouvant altérer les obligations ou la responsabilité des établissements financiers.

La réforme du PCC en fait précisément partie. Elle obligera les banques à faire analyser structurellement les données, et non plus à les stocker de manière passive. La nature de l'obligation est amenée à changer: les banques seront dorénavant tenues de mettre les données à disposition à des fins de traitement.

Il ne s'agit pas d'une nuance technique, mais d'une modification du statut juridique et opérationnel des données bancaires.

Selon la pratique constante de la BCE, une telle mesure devrait lui être soumise sans exception. Dans d'autres États membres – comme l'Espagne, l'Allemagne ou l'Autriche –, même des modifications de moindre importance sont systématiquement soumises à la BCE pour avis.

Il ne s'agit pas d'une simple formule de politesse, cette pratique découle du fragile équilibre entre échange de données et stabilité financière, auquel veille la BCE.

Dans ce dossier, la Belgique n'a toutefois pas consulté la BCE. On n'en trouve aucune trace dans les documents parlementaires, ni de mention dans l'exposé des motifs, ni d'annexe ou encore de résumé de l'avis en question.

Het Raad van State-advies verwijst er evenmin naar en dat terwijl artikel 2 van Besluit 98/415/EG bepaalt dat de ECB “tijdig” moet worden geraadpleegd zodat zij “haar invloed op het wetgevingsproces daadwerkelijk kan uitoefenen”.

“Niet tijdig” is in dit geval een understatement: er is helemaal geen raadpleging geweest.

Waarom is dat problematisch? Omdat het niet enkel een procedurele fout is, maar een juridisch risico.

De rechtspraak van het Hof van Justitie is duidelijk: het niet-inwinnen van een verplicht advies van de ECB maakt een nationale maatregel vernietigbaar. In de arresten C-11/00 Commissie/ECB en C-317/04 Oostenrijk/Commissie wordt bevestigd dat de verplichting tot raadpleging bindend is. Ze waarborgt dat het monetaire en financiële ecosysteem coherent blijft.

Dat het niet is gebeurd, wijst op een gebrekkige voorbereiding of – erger nog – een bewuste poging om de toetsing te vermijden.

2. De rol van de Nationale Bank: technisch expert, moreel waakhond

De Nationale Bank van België (NBB) is niet enkel uitvoerder van monetaire politiek; ze is de wettelijke beheerder van het CAP. Sinds de wet van 8 juli 2018 is zij verantwoordelijk voor het beheer, de beveiliging en de beschikbaarheid van de gegevens. Elke wijziging in de doelstelling of de verwerking van het CAP raakt dus rechtstreeks haar opdracht.

Artikel 322, § 3, WIB 92 bepaalt dat “de Nationale Bank de verwerking uitvoert onder toezicht van de minister van Financiën”. Dat is een gedeelde verantwoordelijkheid: de minister bepaalt de regels, de Bank voert uit, maar mét medebevoegdheid inzake beveiliging, gegevensbescherming en operationele risico's. Een wijziging van dat kader zonder haar advies is dan ook moeilijk te verantwoorden. De Bank is de eerste die weet wat de technische en ethische limieten zijn van de CAP-infrastructuur.

Zij kent de architectuur, de opslaglogica, de encryptie, de toegangslags, de koppelingen met banken via het e-Portal. Zij weet waar de kwetsbaarheden liggen. En

L'avis du Conseil d'État n'y fait pas non plus référence, alors que l'article 2 de la décision 98/415/CE dispose que la BCE doit être consultée en temps utile afin de pouvoir exercer effectivement son influence sur le processus législatif.

Ce serait un euphémisme d'affirmer que la Belgique n'a pas consulté la BCE en temps utile dans ce dossier, dès lors qu'elle ne l'a aucunement consultée.

Cette absence de consultation est problématique, parce qu'elle implique non seulement une erreur de procédure, mais qu'elle comporte également un risque juridique.

Or, la jurisprudence de la Cour de justice est claire à ce sujet: en l'absence de l'avis contraignant de la BCE, toute mesure nationale s'expose à une annulation. Les arrêts C-11/00 Commission/BCE et C-317/04 Autriche/Commission confirment que l'obligation de consultation est contraignante. Elle garantit en effet la cohérence de l'écosystème monétaire et financier.

L'absence d'avis témoigne d'un manque de préparation ou, pire encore, d'une tentative délibérée d'éluder le contrôle de la BCE.

2. Rôle de la Banque nationale: expertise technique et autorité morale

La Banque nationale de Belgique (BNB) n'est pas seulement chargée de la mise en œuvre de la politique monétaire, elle est également la gestionnaire légale du PCC. Depuis l'entrée en vigueur de la loi du 8 juillet 2018, elle est responsable de la gestion, de la sécurisation et de la disponibilité des données. Toute modification apportée à la finalité du PCC ou au traitement des données qu'il contient aura donc une incidence directe sur sa mission.

L'article 322, § 3, du CIR 92 dispose que la BNB effectue ce traitement sous la supervision du ministre des Finances. Il s'agit donc d'une responsabilité partagée: le ministre fixe les règles, la BNB les applique, mais les compétences sont partagées en matière de sécurité, de protection des données et de risques opérationnels. Toute modification apportée à ce cadre juridique sans recueillir l'avis de la BNB est donc difficilement justifiable. La BNB est en effet la mieux placée pour apprécier les limites techniques et éthiques du PCC.

Elle connaît son architecture, la logique de stockage, le cryptage, les journaux d'accès et les connexions avec les banques au moyen du portail électronique. Elle sait

zij weet ook wat de Europese Centrale Bank verwacht qua dataminimalisatie en *purpose limitation*.

Toch werd de NBB niet formeel geraadpleegd. Er is geen spoor van advies, noch in de voorbereidende stukken, noch in de toelichting.

Er is evenmin een passage in het advies van de Raad van State die naar zo'n overleg verwijst.

Dat is bijzonder, want bij de oprichting van het CAP in 2011 én bij de hervorming van 2018 werd de NBB wél geconsulteerd – uitvoerig zelfs. Toen wees ze op de noodzaak van duidelijke begrenzing van doeleinden en op het belang van auditmechanismen.

Die adviezen werden toen overgenomen, nu niet.

Wat betekent dat concreet? Dat de uitvoerder van het systeem geen formeel zeg had in de wijziging van de doelstelling. Dat de instelling die het meest weet over dataveiligheid, risicoanalyse en compatibiliteit met Europese normen buiten spel is gezet. Dat is bestuurlijk niet te verantwoorden. De NBB is niet zomaar een partner, ze is een constitutionele buffer.

Ze beschermt de financiële sector tegen politieke kortsluiting, en de burger tegen technocratische overmoed.

Door haar buiten het proces te houden, heeft de regering een laag van rationele toetsing verloren en dat verlies vertaalt zich onvermijdelijk in zwakke wetgeving.

3. De Inspectie van Financiën: de vergeten poortwachter

Naast de Europese en nationale banken is er nog een waakhond: de Inspectie van Financiën. In het Belgisch administratief bestel heeft zij de taak om elk ontwerp met budgettaire of administratieve impact te toetsen op noodzaak, efficiëntie en proportionaliteit. Artikel 14 van het koninklijk besluit van 16 november 1994 bepaalt dat elk ontwerp van wet met financiële implicaties aan haar moet worden voorgelegd. Het is een klassieke schakel in de begrotingsdiscipline en de controle op bestuurlijke uitgaven. Een systeem van geautomatiseerde datamining op bankrekeningen heeft vanzelfsprekend financiële en administratieve implicaties:

— nieuwe infrastructuur bij de FOD Financiën;

où se trouvent les failles. Et elle connaît par ailleurs les attentes de la Banque centrale européenne en matière de minimisation des données et de limitation des finalités.

La BNB n'a pourtant pas été formellement consultée. On ne trouve en effet aucune trace d'avis, ni dans les documents préparatoires, ni dans l'exposé des motifs.

Aucun passage de l'avis du Conseil d'État ne renvoie en outre à une quelconque concertation.

On peut s'en étonner, puisque lors de la création du PCC en 2011 et lors de la réforme de 2018, la BNB avait bel et bien été consultée, et même de manière approfondie. Elle avait alors souligné la nécessité de délimiter clairement les finalités ainsi que l'importance des mécanismes d'audit.

Ces avis avaient été pris en considération à l'époque, ce qui n'est pas le cas aujourd'hui.

On peut en déduire que le gestionnaire du système n'a pas formellement son mot à dire dans la révision des finalités. Force est également de constater que l'institution qui connaît le mieux la protection des données, l'analyse des risques et la compatibilité avec les normes européennes a été tenue à l'écart. C'est injustifiable sur le plan administratif. La BNB n'est pas un simple partenaire, c'est un "tampon constitutionnel".

Elle protège le secteur financier contre les courts-circuits politiques et les citoyens contre l'impudence technocratique.

En l'écartant du processus législatif, le gouvernement a perdu un niveau de contrôle rationnel, ce qui se traduit inévitablement par un affaiblissement de la législation.

3. Inspection des finances: l'autorité de contrôle oubliée

Outre les banques européennes et nationales, il existe une autre autorité de contrôle, à savoir l'Inspection des finances. Dans le système administratif belge, elle a pour mission d'examiner la nécessité, l'efficacité et la proportionnalité de tout projet ayant une incidence budgétaire ou administrative. L'article 14 de l'arrêté royal du 16 novembre 1994 dispose que tout projet de loi ayant des répercussions financières doit lui être soumis. Il s'agit d'un maillon classique de la discipline budgétaire et du contrôle des dépenses administratives. Un système de *data mining* automatisé des comptes bancaires aura de toute évidence des répercussions financières et administratives:

— nouvelle infrastructure au SPF Finances;

— aanpassing van de CAP-interfaces bij de NBB;

— extra Controlecapaciteit bij de administratie;

— bijkomende verantwoordelijkheden voor de DPO en auditdiensten.

Een inspectieverslag had kunnen aantonen of die middelen voorzien zijn, of de opbrengstprognoses realistisch zijn en of de proportionaliteit tussen investering en verwachte fraudeopbrengst standhoudt. Er is geen spoor van zo'n verslag.

Mogelijk omdat men het project als beleidsneutraal heeft voorgesteld, alsof het enkel een uitvoering van bestaande bevoegdheden was. Maar dat is misleidend.

De uitbreiding naar geautomatiseerde analyse is geen voortzetting, maar een verandering van aard. Het ontbreken van een advies van de Inspectie is dus niet alleen een vormfout, het is een gemiste kans om de kosten-batenbalans transparant te maken.

Waarom werden die adviezen niet gevraagd? Omdat men haast had, omdat de maatregel via een wet diverse bepalingen werd doorgedrukt, met krappe termijnen en zonder aparte nota, omdat men dacht dat een advies tijd zou kosten en tijd politiek ongemak zou brengen.

Maar democratische legitimiteit is niet gebaat bij snelheid; ze is gebaat bij diepgang.

De keuze om drie controlelagen over te slaan, is symptomatisch voor een bestuursstijl waarin efficiëntie boven rede wordt geplaatst. Men spreekt van “modernisering”, maar bedoelt “omzeiling”. Men wil daadkracht tonen, maar vergeet dat daadkracht zonder reflectie slechts lawaai is.

Het goede nieuws is dat herstel nog mogelijk is: de wet is nog niet gestemd en de uitvoeringsbesluiten kunnen nog worden aangepast. De Kamer kan nog een interparlementair verzoek indienen aan de minister om alsnog de adviezen van ECB, NBB en Inspectie van Financiën op te vragen en pas dan beslissen of het CAP – en de

— adaptation des interfaces du PCC à la BNB;

— capacité de contrôle supplémentaire au sein de l'administration;

— nouvelles responsabilités confiées au DPO et aux services d'audit.

Un rapport d'inspection aurait pu déterminer si les moyens envisagés sont disponibles, si les prévisions de recettes sont réalistes et si la proportionnalité entre l'investissement et les recettes attendues de la lutte contre la fraude tient la route. Or, on ne trouve aucune trace d'un tel rapport.

L'absence de ce rapport pourrait s'expliquer par le fait que le projet a été présenté comme politiquement neutre, comme s'il s'agissait simplement d'une mise en œuvre de compétences existantes. Cette vision est toutefois trompeuse.

L'extension du PCC à l'analyse automatisée n'est pas une suite logique, mais elle affecte la nature de la finalité. L'absence d'avis de l'Inspection des finances n'est donc pas seulement un vice de forme, c'est aussi une occasion manquée de rendre transparente l'analyse coûts-bénéfices.

Pourquoi ces avis n'ont-ils pas été recueillis? D'aucuns pourraient invoquer l'urgence et le fait que la mesure a été inscrite dans un projet de loi portant des dispositions diverses avec des délais serrés et sans note distincte, au motif qu'un avis prendrait du temps et que ce laps de temps nuirait à la politique.

Or, ce n'est pas en précipitant les choses que le projet gagnera en légitimité démocratique mais bien en les examinant en profondeur.

Le choix opéré par le gouvernement de passer outre trois niveaux de contrôle est symptomatique d'un mode de gouvernance privilégiant l'efficacité au détriment de la raison. Alors que d'aucuns parlent de “modernisation”, il s'agit en réalité d'un contournement de ces contrôles. Le gouvernement veut faire preuve de dynamisme, mais il oublie que le dynamisme irréfléchi ne sert qu'à faire du bruit.

La bonne nouvelle, c'est qu'il est encore possible de rectifier le tir: le projet de loi n'a pas encore été adopté et les arrêtés d'exécution peuvent encore être modifiés. La Chambre peut encore soumettre une requête interparlementaire au ministre pour qu'il recueille les avis de la BCE, de la BNB et de l'Inspection des finances, et ce

datamining die eraan wordt toegevoegd – werkelijk de richting is die de wetgever wilt inslaan.

— *Het Centraal Aanspreekpunt van rekeningen en financiële contracten (CAP)*

Het CAP is een register dat wordt beheerd door de Nationale Bank van België (NBB).

Het systeem centraliseert de kerninformatie over bankrekeningen, financiële contracten en hun titularissen. Het werd ingevoerd om de overheid in staat te stellen sneller, consistent en veiliger gegevens op te vragen bij financiële instellingen. Het CAP is geen financiële instelling en geen controleorgaan: het is een technisch knooppunt dat gegevens ontvangt, structureert en bewaart. De bedoeling is dat bevoegde overheden, zoals de FOD Financiën of het Openbaar Ministerie, niet langer afzonderlijk alle banken hoeven te contacteren, maar één centraal systeem kunnen raadplegen.

Het juridische fundament van het CAP is de wet van 8 juli 2018 betreffende de organisatie van een centraal aanspreekpunt van rekeningen en financiële contracten (*Belgisch Staatsblad* van 16 juli 2018). Deze wet wordt uitgevoerd door het koninklijk besluit van 23 september 2020. Samen bepalen zij de verplichtingen van de financiële instellingen, de rol van de NBB als beheerder, de toegang van overheidsdiensten en de bewaartermijnen en beveiligingsvereisten.

Het register is geïntegreerd in het netwerk van de NBB, werkt volgens Europese beveiligingsnormen en ondersteunt drie beleidsdoelen:

- efficiëntere fiscale Controle;
- versterking van de strijd tegen witwassen;
- vereenvoudiging van administratieve procedures.

Het CAP kwam er in uitvoering van Europese anti-witwas richtlijnen en internationale normen van de FATF (*Financial Action Task Force*). De derde Europese anti-witwas richtlijn (2005/60/EG) verplichtte lidstaten om systemen op te zetten waarmee bevoegde autoriteiten snel konden weten waar iemand bankrekeningen aanhoudt. België heeft dat volledig omgezet met de wet van 14 april 2011, die het Centraal Aanspreekpunt van

n'est qu'ensuite qu'il sera décidé si le PCC – et le *data mining* qui y est associé – correspond réellement à la direction que le législateur souhaite prendre.

— *Le Point de contact central des comptes et contrats financiers (PCC)*

Le PCC est un registre géré par la Banque nationale de Belgique (BNB).

Le système centralise les informations clés relatives aux comptes bancaires, aux contrats financiers et à leurs titulaires. Il a été mis en place afin de permettre à l'administration de demander des données aux institutions financières de manière plus rapide, plus cohérente et plus sûre. Le PCC n'est ni une institution financière, ni un organe de contrôle: il s'agit d'un "nœud technique" qui reçoit, structure et conserve des données pour que les autorités compétentes, comme le SPF Finances et le ministère public, ne soient plus obligées de contacter séparément toutes les banques mais puissent consulter un système central unique.

Le fondement juridique du PCC est la loi du 8 juillet 2018 portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt (*Moniteur belge* du 16 juillet 2018). Cette loi a été exécutée par l'arrêté royal du 23 septembre 2020. Ensemble, ces actes définissent les obligations des institutions financières, le rôle de la BNB en tant que gestionnaire, l'accès aux services publics, ainsi que les délais de conservation et les exigences en matière de sécurisation.

Le registre a été intégré dans le réseau de la BNB, applique les normes européennes en matière de sécurité et soutient trois objectifs stratégiques:

- optimiser le contrôle fiscal;
- renforcer la lutte contre le blanchiment;
- simplifier les procédures administratives.

Le PCC trouve son origine dans la mise en œuvre des directives européennes anti-blanchiment et des normes internationales du GAFI (*Groupe d'action financière*). La troisième directive européenne anti-blanchiment (2005/60/CE) obligeait les États membres à mettre en place des systèmes permettant aux autorités compétentes de savoir rapidement où un titulaire détient des comptes bancaires. La Belgique a intégralement transposé cette

rekeningen en financiële contracten oprichtte bij de Nationale Bank van België.

De wet van 2011 kwam er in een klimaat van publieke verontwaardiging over offshore structuren en belastingontwijking. In 2008-2009 waren er de LGT-affaire (Liechtenstein) en de eerste SwissLeaks-dossiers. België werd toen door de OESO en de FATF bekritiseerd wegens “gebrekkige transparantie” in haar financiële stelsel. De regering-Di Rupo (2011) engageerde zich om België van de zogeheten grijze lijst van belastingparadijzen te halen.

Later, met de *Panama Papers* (2016), *Paradise Papers* (2017) en *Pandora Papers* (2021), werd het CAP verder versterkt en uitgebreid.

De wet van 8 juli 2018 (verwijzend naar Richtlijn 2016/2258/EU) was rechtstreeks ingegeven door Europese harmonisatie: het ging om de uitvoering van de DAC5-richtlijn, die fiscale autoriteiten toegang moest geven tot antiwitwasdata.

Het CAP werd opgericht om gericht te kunnen zoeken, maar dreigt te evolueren naar een systeem dat zelf zoekt waar iets te vinden valt – dus van gericht toezicht naar algemene surveillance. Het Centraal Aanspreekpunt is geboren uit Europese regelgeving en internationale druk om financiële transparantie te waarborgen. Maar wat begon als een instrument tegen zwarte geldstromen, dreigt uit te groeien tot een permanente infrastructuur van datavertrouwen waarin elke burger stilaan transparanter wordt dan de overheid zelf.

Het oorspronkelijke CAP werd opgericht bij wet 14 april 2011 met als doel artikel 322 van het WIB te wijzen. Een paragraaf 2 werd ingevoerd dat stelde dat wanneer de administratie bij het onderzoek over één of meer aanwijzingen van belastingontduiking beschikt, of wanneer de administratie zich voorneemt om de belastbare grondslag te bepalen, overeenkomstig artikel 341, wordt een bank, een wissel, krediet of spaarinstelling als een derde beschouwd, waarop de bepalingen van paragraaf 1 onverminderd van toepassing zijn. Paragraaf 1 zegt het recht om bijvoorbeeld een derde te horen. In voorkomend geval, dus in geval van aanwijzingen van belastingontduiking, kan de ambtenaar met minstens de graad van adviseur, elke inlichting opvragen die nuttig kan zijn om het bedrag van de belastbare inkomsten van de belastingplichtigen te bepalen.

directive avec la loi du 14 avril 2011, qui a créé le Point de contact central des comptes et contrats financiers auprès de la Banque nationale de Belgique.

La loi de 2011 a vu le jour dans un climat d'indignation de l'opinion publique à l'égard des structures offshore et de l'évasion fiscale. En 2008-2009, il y a eu l'affaire LGT (Liechtenstein) et les premiers dossiers SwissLeaks. La Belgique a alors été critiquée par l'OCDE et le GAFI pour le “manque de transparence” de son système financier. Le gouvernement Di Rupo (2011) s'est alors engagé à faire sortir la Belgique de la liste grise des paradis fiscaux.

Plus tard, suite aux *Panama Papers* (2016), aux *Paradise Papers* (2017) et aux *Pandora Papers* (2021), le PCC a été renforcé et élargi.

La loi du 8 juillet 2018 (qui renvoie à la directive 2016/2258/UE) s'inscrivait directement dans un objectif d'harmonisation européenne: il s'agissait d'exécuter la directive DAC5 censée donner aux autorités fiscales l'accès aux données antiblanchiment.

Si le PCC a été créé afin de pouvoir effectuer des recherches de manière ciblée, il risque aujourd'hui d'évoluer vers un système qui cherche de lui-même là où quelque chose est susceptible d'être trouvé – passant donc d'une surveillance ciblée à une surveillance généralisée. Le Point de contact central est né de la réglementation européenne et de la pression internationale visant à garantir la transparence financière. Mais ce qui était initialement un instrument de lutte contre les flux financiers illégaux risque de se muer en une infrastructure permanente de données dans laquelle chaque citoyen deviendra petit à petit plus transparent que l'autorité elle-même.

Le PCC initial a été créé par la loi du 14 avril 2011 dans le but de modifier l'article 322 du CIR. Un paragraphe 2 a été ajouté. Celui-ci précise que lorsque l'administration dispose dans le cadre de l'enquête d'un ou de plusieurs indices de fraude fiscale [...] ou lorsque l'administration envisage de déterminer la base imposable conformément à l'article 341, un établissement de banque, de change, de crédit ou d'épargne est considéré comme un tiers soumis sans restriction à l'application des dispositions du paragraphe 1^{er}. Le paragraphe 1^{er} prévoit le droit d'entendre des tiers, par exemple. Le cas échéant, c'est-à-dire en cas d'indices de fraude fiscale, un fonctionnaire ayant au moins le titre de conseiller, peut [...] réclamer [...] tout renseignement pouvant être utile pour déterminer le montant des revenus imposables du contribuable.

De ambtenaar mag de machtiging straks verlenen, nadat de ambtenaar die het onderzoek voert, de inlichtingen en gegevens met betrekking tot rekeningen tijdens het onderzoek middels een vraag om inlichtingen en bij die vraag duidelijk heeft aangegeven dat hij de toepassing in artikel 322, § 2, WIB kan vragen indien de belastingplichtige de gevraagde gegevens verborgen houdt of ze weigert te verschaffen.

Nadat de ambtenaar heeft vastgesteld dat het gevoerde onderzoek een eventuele toepassing van artikel 341 uitwijst, of één of meer aanwijzingen van belastingontduiking heeft opgeleverd.

Dat was de initiële bepaling in artikel 322 §§ 2 en 3. En dan in diezelfde wet van april 2011 is er in artikel 333/1 § 2 ingevoerd, waar de spreker een vraag over heeft. In die paragraaf 2 staat het volgende: “de Belastingadministratie bezorgt de minister éénmaal per jaar een verslag dat onder meer volgende informatie bevat: 5. Een globale evaluatie, zowel op technisch vlak als op juridisch vlak, van de wijze waarop de procedure volgens artikel 322 § 2 tot 4 is gevoerd. Dit verslag wordt openbaar gemaakt door de minister van Financiën en overgezonden aan de Kamer van volksvertegenwoordigers.”

Het verslag zou er al moeten zijn sinds 2012 want de wet is in werking getreden sinds 1 juli 2011.

Is dat verslag opgemaakt? Is die evaluatie gebeurd? Wat waren de belangrijkste conclusies? Kunnen de leden van de commissie kopie ontvangen van die evaluatie?

En dan komt de hervorming 2018, de grondige modernisering van het CAP, het Centraal Aanspreekpunt.

Wat waren de belangrijkste vernieuwingen?

- een echte databank;
- uitbreiding naar financiële contracten, leningen, levensverzekeringen;
- strengere veiligheids- en auditnormen;
- verfijning van de regels rond logging en bewaartijden.

De wet van 8 juli 2018 is in werking getreden op 26 juli 2018. Toen is het beslist geweest om het CAP onder te brengen in de schoot van de Nationale Bank om de onafhankelijkheid ten volle te garanderen. Het is de eerste keer dat men sprak van een Centraal Aanspreekpunt van rekeningen en financiële contracten.

Le fonctionnaire peut uniquement accorder l'autorisation après que l'agent qui mène l'enquête a réclamé au cours de l'enquête les informations et données relatives aux comptes, par le biais d'une demande de renseignements [...] et a stipulé clairement à cette occasion qu'il peut requérir l'application de l'article 322, § 2, si le contribuable dissimule les informations demandées ou s'il refuse de les communiquer;

Ou après avoir constaté que l'enquête effectuée implique une application éventuelle de l'article 341 ou qu'elle a fourni un ou plusieurs indices de fraude fiscale.

Telle était la formulation initiale de l'article 322, §§ 2 et 3. Ensuite, la même loi d'avril 2011 a inséré l'article 333/1^{er}, § 2, à propos duquel l'intervenant s'interroge. Le paragraphe 2 dudit article indique ce qui suit: “§ 2. L'administration fiscale fournit une fois par an au ministre un rapport qui contient, entre autres, les informations suivantes: 5° une évaluation globale, tant sur le plan technique que juridique, de la manière dont a été menée la procédure selon l'article 322, §§ 2 à 4. Ce rapport est publié par le ministre des Finances et transmis à la Chambre des représentants.”

Le rapport aurait déjà dû être transmis depuis 2012 car la loi est entrée en vigueur le 1^{er} juillet 2011.

Ce rapport a-t-il été rédigé? Cette évaluation a-t-elle eu lieu? Quelles en étaient les principales conclusions? Les membres de la commission pourraient-ils obtenir une copie de cette évaluation?

Ensuite, il y a lieu la réforme de 2018, la modernisation profonde du point de contact central (PCC).

Quelles étaient les principales innovations?

- une véritable base de données;
- un élargissement aux contrats financiers, aux prêts et aux polices d'assurance-vie;
- des normes plus strictes en matière de sécurité et d'audit;
- des règles plus claires en matière d'enregistrement et de délais de conservation.

La loi du 8 juillet 2018 est entrée en vigueur le 26 juillet 2018. À l'époque, il avait été décidé de placer le PCC dans le giron de la Banque nationale afin de garantir pleinement son indépendance. C'est la première fois qu'apparaît la dénomination de Point de contact central des comptes et contrats financiers.

De heer Van Quickenborne kondigt aan dat hij een amendement zal indienen om voortaan niet meer te spreken over het CAP, maar over het *money control* als nieuwe naam voor het CAP dat huisvest is bij de Nationale Bank van België.

De spreker geeft aan dat niet alleen bankrekeningen onder het CAP vallen, maar ook heel wat financiële contracten. Daarnaast is het zo dat het CAP gevoed wordt met informatie die afkomstig is van wat men noemt de informatieplichtigen. Dat zijn in de eerste plaats de kredietinstellingen, de banken, maar ook de beursvennootschappen, de betalingsinstellingen, de instellingen voor elektronisch geld, de in België gevestigde personen die beroepshalve verrichtingen uitvoeren voor de contantenaankoop of verkoop van deviezen in baar geld, of met cheques in deviezen, de verzekeringsondernemingen, de ondernemingen gespecialiseerd in financieringshuur, de kredietgevers, zoals bepaald in het Wetboek economisch recht, en ook b-post. B-post beschikt door de uitgifte van elektronisch geld en de financiële postdiensten ook over die informatie. Al deze instellingen moeten het CAP voeden.

3. Vergadering van 5 november 2025

De heer Van Quickenborne (Open-Vld) gaat dieper in op artikel 4 van de wet van 8 juli 2018 dat handelt over de verplichtingen van de informatieplichtigen. Het gaat dan bijvoorbeeld over de banken die de rekeningnummers en ook saldi moeten meedelen aan het CAP. Deze melding moet onverwijld gebeuren voor verschillende transacties zoals bij de opening van een rekening maar ook bij het afsluiten van een rekening.

Ook als er contanten worden gestort of afgehaald door een cliënt wordt dit beschouwd als een financiële verrichting en moet dat dus ook worden meegedeeld aan het CAP.

Daarnaast moeten ook de financiële contracten aan het CAP worden meegedeeld. Daaronder vallen bijvoorbeeld de verhuur van kluizen en levensverzekeringen van het type tak 21, 23, 25 en 26. Dit is uiteraard van belang omdat op al deze informatie datamining kan worden toegepast. De resultaten van deze datamining kunnen dan door de fiscus worden aangewend om desgevallend fraude op te sporen.

Verder dienen ook de hypothecaire kredieten, verkopen op afbetaling, leasingovereenkomsten, leningsovereenkomsten en kredietopeningen te worden gemeld aan het CAP.

M. Van Quickenborne annonce qu'il présentera un amendement tendant à remplacer la dénomination du PCC, qui est hébergé au sein de la Banque nationale de Belgique, par "*money control*".

L'intervenant indique que non seulement les comptes bancaires, mais également de nombreux contrats financiers relèvent du PCC. En outre, le PCC est alimenté par des informations provenant de ce que l'on appelle les "redevables d'information". Il s'agit en premier lieu des établissements de crédit, des banques, mais également des sociétés de bourse, des établissements de paiement, des établissements de monnaie électronique, des personnes établies en Belgique qui effectuent à titre professionnel des opérations d'achat ou de vente de devises en espèces ou par chèques en devises, des entreprises d'assurances, des entreprises spécialisées dans la location-financement, des prêteurs, tels que définis dans le Code de droit économique, ainsi que b-post. B-post dispose également de ces informations grâce à l'émission de monnaie électronique et à la fourniture de services financiers postaux. Toutes ces institutions doivent alimenter le PCC.

3. Réunion du 5 novembre 2025

M. Van Quickenborne (Open-Vld) se penche sur l'article 4 de la loi du 8 juillet 2018, qui concerne les obligations des redevables d'information. Il s'agit, par exemple, des banques qui doivent communiquer les numéros de compte ainsi que les soldes au PCC. Cette communication doit avoir lieu sans délai pour différentes transactions, telles que l'ouverture ou la fermeture d'un compte.

Le versement et le retrait d'espèces par un client sont également considérés comme une opération financière, qu'il faut donc communiquer au PCC.

Les contrats financiers doivent aussi être communiqués au PCC. Cela concerne, par exemple, la location de coffres et les assurances-vie relevant des branches 21, 23, 25 et 26. Il s'agit naturellement d'une précision importante, étant donné que toutes ces informations pourront être utilisées à des fins de *data mining* et que l'administration fiscale pourra ensuite s'appuyer sur les résultats de ce *data mining* pour détecter une fraude éventuelle.

En outre, les crédits hypothécaires et les conventions de vente à tempérament, de location-financement et de prêt à tempérament, ainsi que les ouvertures de crédit, doivent être communiqués au PCC.

In de wet van 8 juli 2018 zijn er in tegenstelling tot de amendementen nrs. 17 tot 22 van de regering (DOC 56 0963/005) wel koninklijke besluiten voorzien om die wet uit te voeren. Zo bepaalt de Koning bijvoorbeeld het minimumbedrag, waaronder financiële verrichtingen waarbij contanten betrokken zijn, niet moeten worden meegedeeld. Deze grens ligt op 3000 euro aan contanten. De regering gaat er dus blijkbaar vanuit dat iemand die voor een bedrag van 3000 euro of meer contante betalingen doet dus eigenlijk een potentiële fraudeur is.

Artikel 5 van de wet van 8 juli 2018 bepaalt dat de mededeling van alle gegevens aan het CAP enkel via elektronische weg kan plaatsvinden. Ook daar is er een uitvoeringsbesluit dat zegt hoe dat moet gebeuren.

Artikel 5 bepaalt ook welke gegevens de informatieplichtigen aan hun cliënten moeten melden:

- de wettelijke verplichting in hoofde van de informatieplichtigen om bepaalde gegevens aan het CAP mee te delen;

- het feit dat deze gegevens in het CAP worden opgeslagen;

- de naam en het adres van het CAP;

- de doeleinden van de verwerking door het CAP, alsook van het feit dat de persoonsgegevens opgeslagen in het CAP onder meer gebruikt mogen worden in het kader van een fiscaal onderzoek, van de opsporing van strafbare inbreuken en van de bestrijding van het witwassen van geld en van de financiering van het terrorisme en van de zware criminaliteit, mits de door de wet opgelegde voorwaarden worden nageleefd;

- het recht van de betrokkene tot inzage bij de NBB van de persoonsgegevens die door het CAP op zijn naam zijn geregistreerd;

- het recht van de betrokkene, bij voorkeur rechtstreeks bij de betrokken informatieplichtige uit te oefenen, tot verbetering en verwijdering van onjuiste gegevens die door het CAP op zijn of haar naam zijn geregistreerd; en

- de bewaartermijnen van de in het CAP opgeslagen gegevens.

Hierbij stelt de spreker zich de vraag of de minister de banken ook zal verplichten om mee te delen aan alle klanten dat er voortaan zoiets zal bestaan als *money control*, namelijk dat de banken hun cliënten moeten

Contrairement aux amendements n^{os} 17 à 22 du gouvernement (DOC 56 0963/005), la loi du 8 juillet 2018 prévoit des arrêtés royaux d'exécution. Ainsi, le Roi détermine, par exemple, le montant minimum en dessous duquel des transactions financières impliquant des espèces ne doivent pas être communiquées au PCC. Ce montant limite est fixé à 3000 euros en espèces. Le gouvernement part donc manifestement du principe qu'une personne qui effectue des paiements en espèces d'un montant supérieur ou égal à 3000 euros est, en réalité, un fraudeur potentiel.

La loi du 8 juillet 2018 dispose en son article 5 que la communication de toutes données au PCC ne peut avoir lieu que par voie électronique. À cet égard également, un arrêté d'exécution détermine les modalités de cette communication.

L'article 5 mentionne aussi les informations que les redevables d'information doivent fournir à leurs clients, à savoir:

- l'obligation légale qui incombe aux redevables d'information de communiquer certaines informations au PCC;

- l'enregistrement de ces données dans le PCC;

- le nom et l'adresse du PCC;

- les finalités du traitement effectué par le PCC, ainsi que le fait que les données personnelles enregistrées dans le PCC peuvent entre autres être utilisées dans le cadre d'une enquête fiscale, de la recherche d'infractions pénalement sanctionnables et de la lutte contre le blanchiment de capitaux et contre le financement du terrorisme et de la grande criminalité, dans le respect des conditions imposées par la loi;

- le droit de l'intéressé de prendre connaissance auprès de la BNB des données personnelles enregistrées à son nom par le PCC;

- le droit de l'intéressé à la rectification et à la suppression des données inexacts enregistrées à son nom par le PCC, droit qui doit de préférence être exercé directement auprès du redevable d'information concerné, et

- les délais de conservation des données enregistrées dans le PCC.

À ce propos, l'intervenant se demande si les banques seront aussi tenues d'informer tous leurs clients qu'il existera désormais une sorte de contrôle des flux financiers et que leurs données seront peut-être utilisées à

informerende dat hun gegevens mogelijks zullen worden gebruikt voor *datamining*, voor *datascreening* en voor profilering. Hierover staat niets vermeld in de betrokken amendementen van de regering, noch in de begeleidende verantwoording. Mag men er dan van uitgaan dat de banken niet verplicht zullen zijn om hun cliënten daarvan op de hoogte te brengen? Als dat zo is, staat dat dan niet totaal in contrast met de verplichtingen die zijn opgenomen in artikel 5 van de wet van 8 juli 2018?

Artikel 6 van de wet van 8 juli 2018 bepaalt welke informatiegerechtigden bij het CAP geregistreerde gegevens kunnen opvragen. De spreker verwondert er zich over dat de informatie die door het CAP aan de informatiegerechtigden wordt overgemaakt, niet wordt beperkt tot de gevraagde gegevens. Het CAP geeft blijkbaar telkens toegang tot alle gegevens die over een bepaalde natuurlijke persoon of rechtspersoon in het CAP zijn opgenomen. Een notaris zal dus bijvoorbeeld niet alleen de gegevens kunnen inkijken die hij nodig heeft, maar ook alle andere gegevens die met betrekking tot die (rechts)persoon in het CAP zijn opgenomen.

De informatiegerechtigden zijn onder meer de FOD Financiën, de Vlaamse belastingdienst (VLABEL), de gerechtsdeurwaarders, de notarissen, de Cel voor financiële informatieverwerking (CFI). Deze personen hebben allemaal toegang tot het CAP, uiteraard bij vermoeden van fraude of in andere gevallen. Ook elke persoon die in het CAP is opgenomen, kan zijn eigen gegevens in het CAP consulteren. Daarnaast kunnen ook de personeelsleden van de Nationale Bank het CAP consulteren, maar enkel natuurlijk om antwoorden te geven op de aanvragen tot informatie. De heer Van Quickenborne besluit dat de toegang tot het CAP vandaag dus zeer beperkt is en ook zeer sterk is gereguleerd. Als het CAP wordt opengesteld voor *datamining*, dan is het risico op informatiedeling veel groter dan wat vandaag het geval is.

Artikel 8 van de wet van 8 juli 2018 bepaalt ook dat iedere in het CAP geregistreerde persoon op verzoek gericht aan de NBB, hetzij schriftelijk, hetzij via diens website, de lijst meegedeeld krijgt van alle instellingen, overheden en personen aan wie zijn gegevens tijdens de zes kalendermaanden voorafgaand aan de datum van zijn aanvraag werden meegedeeld. Echter wordt de NBB echter vrijgesteld van de verplichting om de lijst mee te delen van de instellingen, overheden en personen waarvan de aanvragen om informatie omtrent de betrokkene ingegeven werden door overwegingen die verband houden met de nationale veiligheid, met de landsverdediging, met de openbare veiligheid of met de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging

des fins de *datamining*, de *datascreening* et de profilage. Rien n'est précisé à ce sujet dans les amendements concernés du gouvernement, ni dans leur justification. Peut-on dès lors considérer que les banques ne seront pas obligées d'en informer leurs clients? Dans l'affirmative, ne serait-ce pas totalement contradictoire avec les obligations mentionnées dans l'article 5 de la loi du 8 juillet 2018?

L'article 6 de la loi du 8 juillet 2018 précise quelles personnes habilitées à recevoir l'information peuvent demander à consulter des données enregistrées dans le PCC. L'intervenant s'étonne que les informations transmises à ces personnes par le PCC ne se limitent pas aux données demandées. Le PCC donne apparemment chaque fois accès à toutes les données concernant une certaine personne physique ou morale qui sont enregistrées dans sa base de données. Ainsi, par exemple, un notaire aura accès non seulement aux données dont il a besoin, mais aussi à toutes les autres données enregistrées dans le PCC qui concernent la personne (morale) en question.

Les personnes habilitées à recevoir l'information sont, entre autres, le SPF Finances, l'administration fiscale flamande (VLABEL), les huissiers de justice, les notaires et la Cellule de traitement des informations Financières (CTIF). Elles peuvent toutes avoir accès au PCC, naturellement en cas de présomption de fraude ou dans d'autres situations. Toute personne enregistrée dans le PCC peut aussi consulter ses propres données figurant dans le PCC. Par ailleurs, les membres du personnel de la Banque nationale peuvent également consulter le PCC, mais bien entendu uniquement pour répondre aux demandes d'information. M. Van Quickenborne en conclut que l'accès au PCC est très limité et très réglementé à l'heure actuelle. Si le PCC est rendu accessible à des fins de *data mining*, le risque de partage d'informations sera bien plus élevé qu'aujourd'hui.

L'article 8 de la loi du 8 juillet 2018 prévoit aussi que toute personne enregistrée dans le PCC reçoit, sur demande adressée à la BNB par écrit ou via son site web, communication de la liste de tous les organismes, autorités et personnes qui ont reçu communication de ses données au cours des six mois calendrier précédant la date de sa demande. La BNB est toutefois exemptée de l'obligation de communiquer la liste des organismes, autorités et personnes dont les demandes d'information portant sur la personne concernée étaient motivées par des considérations qui relèvent de la sécurité nationale, de la défense nationale, de la sécurité publique ou de la prévention et la détection d'infractions pénales ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre

van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid. Dat betekent dus eigenlijk dat als iemand het CAP consulteert voor zichzelf, dat hij in die consultatie niet kan zien welke autoriteit of autoriteiten die gegevens hebben geconsulteerd. Waarom kan men vandaag, als men het CAP consulteert, niet zien wie of welke autoriteit, zijn of haar gegevens heeft geconsulteerd? Voor het UBO-register, en zelfs voor de databank van de staatsveiligheid is dat bijvoorbeeld wel het geval. Heeft de minister de intentie om de transparantie op dit vlak te verbeteren?

Artikel 8 van de wet van 8 juli 2018 bepaalt ook dat iedere informatiegerechtigde verantwoordelijk is voor de naleving van de wetgeving krachtens dewelke de informatie uit het CAP wordt opgevraagd. De informatiegerechtigden zijn dus verantwoordelijk om enkel die gegevens te consulteren die ze mogen consulteren, en de andere gegevens die ze weliswaar krijgen, mogen ze eigenlijk niet zien. Zo werkt het systeem blijkbaar vandaag. Kan de minister bevestigen dat het vandaag effectief zo is dat het CAP alle gegevens met betrekking tot één persoon of rechtspersoon aan een informatiegerechtigde bezorgt, ook al heeft die informatiegerechtigde niet het recht om bepaalde gegevens te bekijken?

Artikel 8, § 2, 4°, van de wet van 8 juli 2018 stipuleert dat de informatiegerechtigde verantwoordelijk is voor het feit dat de vertrouwelijkheid van de van het CAP verkregen informatie bewaard blijft en dat hij deze informatie niet verder gebruikt, verwerkt of verspreidt voor doeleinden die niet verenigbaar zijn met de finaliteit waarvoor hij deze informatie initieel aan het CAP opgevraagd heeft.

Artikel 10 van de wet van 8 juli 2018 bepaalt dat de NBB bij provisie wordt vergoed voor alle kosten die ze draagt wegens de inrichting, de werking en het onderhoud van het CAP. Kan de minister aangeven hoeveel deze vergoeding precies bedraagt? Wat zijn die kosten en wie betaalt die kosten? Zijn dat de informatiegerechtigden? Zijn dat de informatieplichtigen? Of allebei?

Artikel 11 van de wet van 8 juli 2018 gaat over de aansprakelijkheid van de NBB. Het artikel bepaalt dat de NBB, de leden van haar organen en haar personeelsleden niet burgerlijk aansprakelijk zijn voor fouten of nalatigheden begaan in het kader van de uitoefening van deze wettelijke opdracht, behalve in geval van bedrog of opzettelijke of zware fout of nalatigheid. Stel dat er een fout gebeurt waarbij gegevens die het CAP verzamelt toch publiek worden gemaakt door *phishing*, door een intrusie, door nalatigheid, dus niet door bedrog,

les menaces pour la sécurité publique et la prévention de telles menaces. Cela signifie donc en réalité qu'une personne qui consulte ses propres données dans le PCC ne peut pas voir à cette occasion quelle personne ou quelle autorité a consulté ses données. Pourquoi n'est-ce pas possible, alors que cette information peut être obtenue à propos du registre UBO et même de la base de données de la Sûreté de l'État, par exemple? Le ministre a-t-il l'intention d'accroître la transparence dans ce domaine?

L'article 8 de la loi du 8 juillet 2018 dispose également que chaque personne habilitée à recevoir l'information est responsable du respect de la législation en vertu de laquelle les informations sont demandées au PCC. Les personnes habilitées à recevoir l'information ont donc la responsabilité de consulter uniquement les données qu'elles sont autorisées à consulter et non les autres données qui leur sont transmises. C'est apparemment ainsi que fonctionne le système aujourd'hui. Le ministre peut-il confirmer qu'à l'heure actuelle, le PCC transmet bel et bien toutes les données relatives à une personne physique ou morale à une personne habilitée à recevoir l'information, même si cette dernière n'a pas le droit de consulter certaines données?

L'article 8, § 2, 4°, de la loi du 8 juillet 2018 précise que la personne habilitée à recevoir l'information a la responsabilité de garantir que la confidentialité des informations obtenues du PCC est sauvegardée et que ces informations ne sont pas ensuite utilisées, retraitées ou diffusées par elle à des fins non compatibles avec la finalité pour laquelle elle les a initialement demandées au PCC.

L'article 10 de la loi du 8 juillet 2018 prévoit que la BNB est remboursée par provision pour tous les frais que cette dernière encourt du fait de l'installation, du fonctionnement et de la maintenance du PCC. Le ministre peut-il préciser le montant exact de ce remboursement? Quelle est la nature de ces frais et à qui incombent-ils? Les personnes habilitées à recevoir l'information, celles redevables d'information ou les deux?

L'article 11 de la loi du 8 juillet 2018 traite de la responsabilité de la BNB. L'article prévoit que la BNB, les membres de ses organes et les membres de son personnel n'encourent aucune responsabilité civile en raison de fautes ou négligences commises dans l'exercice de cette mission légale, sauf en cas de dol ou de faute ou négligence intentionnelle ou lourde. Supposons toutefois qu'une erreur survienne et que des données collectées par le PCC soient malgré tout rendues publiques à la suite d'un hameçonnage, d'une

niet door zware fout, niet door opzettelijke fout. Wie is in dat geval dan verantwoordelijk? Zeker met het oog op de uitbreiding van het CAP en de datamining die erop zal worden toegepast is het belang om te weten wie de verantwoordelijkheid draagt.

Artikel 13 van de wet van 8 juli 2018 bepaalt dat de Administratie van de Thesaurie belast is met de controle op de werking van het CAP. Indien zij een inbreuk op de verplichtingen vaststelt, kan de Administratie van de Thesaurie, na kennis te hebben genomen van de verweermiddelen van de informatieplichtige en, in voorkomend geval, na deze laatste op diens verzoek te hebben gehoord, een administratieve geldboete aan de overtreder opleggen. Het basisbedrag van de administratieve geldboete bedraagt minstens 50.000 euro en hoogstens 1.000.000 euro. Kan de minister aangeven hoeveel boetes de Administratie van de Thesaurie al heeft opgelegd sinds het CAP werd opgericht in 2018? Stel dat er in de toekomst iets verkeerd loopt met de datamining die op het CAP wordt toegepast, wie zal daar dan de verantwoordelijkheid voor dragen?

De spreker verwijst naar het advies van de Gegevensbeschermingsautoriteit (GBA) op de regeringssamendementen (DOC 56 0963/005, p. 76 en volgende) waarin geopperd wordt dat de toepassing van de datamining op het CAP een groot risico inhoudt op schending van de privacy. Wie zal er in dat geval de verantwoordelijkheid dragen? De heer Van Quickenborne begrijpt niet waarom de minister deze belangrijke wijziging van het CAP snel met een aantal regeringssamendementen wenst door te drukken. Waarom werd deze wijziging niet ingediend als een afzonderlijk wetsontwerp? Alleszins vergt dergelijke wijziging een grondig parlementair debat. De spreker betreurt dat vele commissieleden niet lijken te beseffen welke negatieve impact de voorgestelde wijziging zal hebben.

Het CAP werd opgericht bij de wet van 8 juli 2018 onder de toenmalige minister van Financiën, de heer Johan Van Overtveldt en werd ondertussen 8 keer gewijzigd. Het CAP is destijds opgezet geweest voornamelijk voor fiscale doeleinden maar is later geëvolueerd tot een dynamische databank. Vandaag kan het CAP worden gebruikt als een instrument in onder meer de strijd tegen het witwassen van geld, tegen de financiering van terrorisme, tegen de zware criminaliteit en tegen belastingontduiking. Dat zijn eigenlijk de verschillende doelstellingen op dit ogenblik.

Naast de in België bestaande rekeningen en financiële contracten bevat het CAP ook de buitenlandse rekeningen van in België aan de personenbelasting onderworpen natuurlijke personen.

intrusion ou d'une négligence, sans qu'il s'agisse de dol, de faute grave ni de faute intentionnelle. Qui en assumerait la responsabilité? Cette question est d'autant plus importante compte tenu de l'extension du PCC et du recours au *data mining*.

L'article 13 de la loi du 8 juillet 2018 prévoit que l'Administration de la Trésorerie est chargée du contrôle du fonctionnement du PCC. Lorsqu'elle constate une infraction aux obligations, l'Administration de la Trésorerie peut, après avoir pris connaissance des moyens de défense du redevable d'information et, le cas échéant, après l'avoir entendu à sa demande, imposer une amende administrative à l'auteur de l'infraction. Le montant de base de cette amende s'élève au minimum à 50.000 euros et au maximum à 1.000.000 euros. Le ministre peut-il indiquer combien d'amendes l'Administration de la Trésorerie a déjà infligées depuis la création du PCC en 2018? Supposons par ailleurs qu'un incident survienne à l'avenir dans le cadre du *data mining* appliqué au PCC: qui en assumerait la responsabilité?

L'intervenant fait référence à l'avis de l'Autorité de protection des données (APD) relatif aux amendements du gouvernement (DOC 56 0963/005, p. 76 et suivantes) dans lequel il est suggéré que l'application du *data mining* au PCC présente un risque important de violation de la vie privée. Dans ce cas, qui en serait responsable? M. Van Quickenborne ne comprend pas pourquoi le ministre veut faire adopter à la hâte cette modification majeure du PCC au moyen de plusieurs amendements du gouvernement. Pourquoi cette modification n'a-t-elle pas été présentée sous la forme d'un projet de loi distinct? Une telle mesure nécessite en tout cas un débat parlementaire approfondi. L'intervenant déplore que de nombreux membres sous-estiment manifestement l'impact négatif potentiel de cette modification.

Le PCC a été créé par la loi du 8 juillet 2018 sous l'autorité du ministre des Finances de l'époque, M. Johan Van Overtveldt, et a été modifié à huit reprises depuis lors. À l'origine, le PCC avait été principalement conçu à des fins fiscales, avant d'évoluer vers une banque de données dynamique. Aujourd'hui, le PCC peut être utilisé comme un instrument dans le cadre de la lutte contre le blanchiment d'argent, le financement du terrorisme, la criminalité grave et la fraude fiscale. Il s'agit en fait de ses différents objectifs à l'heure actuelle.

Outre les comptes et contrats financiers existant en Belgique, le PCC contient également les comptes étrangers des personnes physiques assujetties à l'impôt des personnes physiques en Belgique.

Het doel van het CAP was dus om informatie snel ter beschikking te stellen van informatiegerechtigden waaronder de FOD Financiën en VLABEL. VLABEL heeft toegang tot het CAP voor de controle en de inning van fiscale en niet-fiscale ontvangsten. Daarnaast is er ook toegang tot het CAP voorzien voor de procureur des Konings, de onderzoeksrechter of de rechtbank, voor de opsporing en vervolging van bepaalde strafrechtelijke inbreuken. Verder is er ook toegang voorzien voor het Centraal Orgaan voor de Inbeslagneming en Verbeurdverklaring (COIV) voor het solvabiliteitsonderzoek, voorafgaand aan de invordering van door het gerecht inbeslaggenomen sommen. Daarnaast is er ook toegang voorzien voor de inlichting- en veiligheidsdiensten. Ook de deurwaarders hebben toegang voor het bevel tot conservatoir beslag. De notarissen hebben eveneens toegang voor de opmaak van de aangifte van een nalatenschap. Ook het CFI heeft toegang en zelfs de Administratie van de Thesaurie, in het kader van de naleving van de financiële sancties, die werden opgelegd in het kader van een sanctieregime. Tot slot zullen in de toekomst ook het RIZIV en Paradigm, de informaticadienst van het Brussels Hoofdstedelijk Gewest toegang krijgen tot het CAP.

Het CAP wordt gevoed door informatie van informatieplichtigen zoals de banken en de beursvennootschappen. Ook de kredietgevers moeten die informatie doorgeven, dus dit geldt blijkbaar niet voor de mobiliseringsinstellingen. Mobiliseringsinstellingen zijn blijkbaar geen kredietgevers volgens het wetboek Economisch recht. Het feit dat zij in het kader van een mobilisering, een hypothecaire schuldvordering in volle eigendom overnemen, maakt van hen professionele crediteuren, maar geen professionele uitleners. Zelf mogen ze immers geen leningen aan derden toestaan.

De gegevens die aan het CAP moeten worden doorgegeven zijn dus de nummers en periodieke saldo's van de bank- en betaalrekeningen van de cliënten in België en de volmachten op die rekeningen. Ook bepaalde voor deze cliënten in België uitgevoerde financiële verrichtingen waarbij contanten zijn betrokken moeten aan het CAP worden gemeld. Het feit dat er contant geld wordt afgehaald dient dus ook te worden gemeld aan het CAP. Op al deze gegevens zal dus voortaan datamining worden toegepast. Het gaat dus niet alleen om money control maar ook om cash control.

Verder zijn dus ook de fameuze financiële contracten opgenomen in het CAP en ook het periodieke globaliseerde bedrag van die contracten. Als je een Tak 21 contract hebt, zal het bedrag dat je daarin hebt geïnvesteerd ook in het CAP opgenomen zijn.

L'objectif du PCC était donc de mettre rapidement l'information à la disposition des personnes habilitées, telles que le SPF Finances et VLABEL, ce dernier y ayant accès pour le contrôle et le recouvrement des recettes fiscales et non fiscales. L'accès au PCC est également prévu pour le procureur du Roi, le juge d'instruction ou le tribunal, afin de détecter et de poursuivre certaines infractions pénales. L'Organe central pour la saisie et la confiscation (OCSC) peut également consulter le PCC en vue de mener des enquêtes de solvabilité préalables au recouvrement de sommes saisies par la Justice. Les services de renseignement et de sécurité peuvent, eux aussi, le consulter. Par ailleurs, les huissiers peuvent y accéder pour l'ordonnance des saisies conservatoires, et les notaires pour l'établissement des déclarations de succession. La CTIF dispose aussi d'un accès au PCC, tout comme l'Administration de la Trésorerie, dans le cadre du respect des sanctions financières imposées par un régime de sanctions. Enfin, à l'avenir, l'INAMI et Paradigm, le service informatique de la Région de Bruxelles-Capitale disposeront également d'un accès.

Le PCC est alimenté par les informations transmises par les redevables d'information, telles que les banques et les sociétés de bourse. Les prêteurs sont également tenus de fournir ces informations, mais cela ne semble pas s'appliquer aux organismes de mobilisation. Selon le Code de droit économique, ces derniers ne sont en effet pas considérés comme des prêteurs. Le fait qu'ils reprennent, dans le cadre d'une mobilisation, une créance hypothécaire en pleine propriété les qualifie de créanciers professionnels, mais pas de prêteurs professionnels, puisqu'ils ne sont pas autorisés à accorder des prêts à des tiers.

Les données à communiquer au PCC sont donc les numéros et soldes périodiques des comptes bancaires et de paiement des clients établis en Belgique, ainsi que les mandats liés à ces comptes. Certaines opérations financières effectuées pour ces clients établis en Belgique et impliquant des espèces doivent aussi être notifiées au PCC. Les retraits d'espèces doivent donc également être notifiés au PCC. Toutes ces données seront donc désormais soumises à l'exploration de données. Il ne s'agira donc pas seulement de contrôler les opérations financières, mais aussi de contrôler les opérations impliquant des espèces.

Par ailleurs, les fameux contrats financiers sont donc aussi enregistrés dans le PCC, de même que leur montant globalisé périodique. Autrement dit, si vous possédez un contrat de la branche 21, le montant que vous y avez investi sera aussi enregistré dans le PCC.

De gegevens in het CAP worden dynamisch beheerd in die zin dat er om de maand informatie wordt gecorrigeerd. De saldi worden twee maal per jaar aangepast.

In zijn advies over de regeringsamendementen (DOC 56 0963/005) wijst de GBA op het probleem dat de fiscus eigenlijk een kopie van het CAP aan datamining zal onderwerpen. De GBA heeft gewaarschuwd voor het feit dat de kopie op een bepaald moment al achterhaald kan zijn. Waarom heeft de minister de suggestie van de GBA om real-time toegang te geven tot het CAP niet opgevolgd? Wanneer is in het CAP te zien dat iemand een rekening heeft geopend? Betekent dynamisch beheer dat dat in het CAP al te zien is onmiddellijk nadat de rekening werd geopend?

Wat betekent money control op de bankrekeningen concreet? Concreet betekent dit dat het IBAN-nummer van die rekening en ook de identiteit van de cliënt in het CAP wordt vermeld, maar ook de toekenning en de intrekking van de volmachten op die rekeningen. De mededeling betreft het nummer van de bankrekening, maar blijkbaar niet de precieze aard van de rekening.

De saldi van de rekeningen worden twee maal per jaar vastgelegd, namelijk op 30 juni en 31 december. Blijkbaar zouden er mensen zijn die kort voor die twee data hun rekeningen doen verminderen om ze dan kort na die data terug te verhogen. Heeft de minister kennis van dit fenomeen en wat zijn desgevallend de implicaties daarvan?

Een bankrekening is wat vermeld staat in, uiteraard de wet op het CAP en ook de uitvoeringsbesluiten, een specifieke onderverdeling in het boekhoudplan van een krediet dat in België tot stand is gekomen ten gevolge van het sluiten van een bancaire of financiële overeenkomst met haar cliënt. Dus die bankrekening behoort daartoe. Opvallend is dat rekeningen die niet onder deze definitie vallen, niet als bankrekening aan het CAP moeten worden meegedeeld. Hoe zit het dan bijvoorbeeld met een termijnrekening? Zit een termijnrekening in het CAP of niet? Of wordt een termijnrekening aanzien als een financieel contract, dat sowieso moet worden meegedeeld aan het CAP? Een termijnrekening die rechtstreeks gecrediteerd of gedebiteerd kan worden naar een betalingsopdracht moet blijkbaar ook meegedeeld worden aan het CAP. Kan de minister dat bevestigen?

Blijkbaar gaat het over termijnrekeningen die een interbancaire fondsoverdracht met zich meebrengen of een afgifte of opname van contanten en die de mogelijkheid bieden inkomsten te ontvangen. Maar termijnrekeningen

Les données contenues dans cette base de données sont gérées de manière dynamique, en ce sens que ces informations y sont corrigées tous les mois. Les soldes y sont actualisés deux fois par an.

Dans son avis sur les amendements présentés par le gouvernement (DOC 56 0963/005), l'APD souligne le problème posé par le fait que le fisc soumettra en réalité une copie du PCC à l'exploration de données. L'APD a mis en garde contre le fait que cette copie pourrait, à un certain moment, déjà ne plus être d'actualité. Pourquoi le ministre n'a-t-il pas donné suite à la suggestion de l'APD de permettre l'accès en temps réel au PCC? Combien de temps après son ouverture un compte figurera-t-il dans le PCC? La gestion dynamique signifie-t-elle que cette information est consultable dans le PCC immédiatement après l'ouverture dudit compte?

Qu'implique concrètement le contrôle des opérations financières appliqué aux comptes bancaires? Que les numéros IBAN de ces comptes et l'identité des clients sont renseignés dans le PCC, mais aussi les octrois et les retraits des mandats sur ces comptes. La notification concerne le numéro du compte bancaire, mais visiblement pas la nature précise de ce compte.

Les soldes des comptes sont relevés deux fois par an, les 30 juin et 31 décembre. Visiblement, certaines personnes diminueraient le montant de leur compte avant ces deux dates, pour le réaugmenter juste après. Le ministre a-t-il connaissance de ce phénomène? Et quelles en sont les implications?

Par compte bancaire, on entend toute subdivision spécifique dans le plan comptable d'un établissement de crédit, créée en Belgique suite à la conclusion d'un contrat bancaire ou financier avec son client. Cette notion est évidemment définie dans la loi relative au PCC, mais aussi dans ses arrêtés d'exécution. Cela signifie donc que les comptes bancaires relèvent du champ d'application de cette notion. Il est toutefois surprenant de constater que les comptes qui ne relèvent pas de ce champ d'application ne doivent pas être notifiés au PCC au titre de compte bancaire. *Quid* alors d'un compte à terme, par exemple? Ce compte est-il renseigné dans le PCC? Ou bien est-il considéré comme un contrat financier, qui doit dans tous les cas être notifié au PCC? Un compte à terme qui peut être crédité ou débité directement à l'occasion d'un ordre de paiement doit visiblement aussi être notifié au PCC. Le ministre pourrait-il le confirmer?

Il s'agirait visiblement des comptes à terme impliquant un transfert de fonds interbancaire ou la remise ou le retrait d'espèces et permettant la perception de revenus. Mais les comptes à terme qui n'offrent pas

die deze mogelijkheden niet bieden, omdat interesten bijvoorbeeld niet rechtstreeks worden gekapitaliseerd, maar eerst worden gestort op de rekening courant, zijn dat dan wel bankrekeningen? Moet dit soort termijnrekeningen met andere woorden worden gemeld aan het CAP?

In de regeringsamendementen staat te lezen dat de effectenrekeningen zullen worden toegevoegd aan het CAP. Maar blijkbaar vallen effectenrekeningen vandaag al onder het CAP, omdat het gaat om financiële contracten. Normaliter vallen effectenrekeningen niet onder de definitie van een bankrekening, ze worden wel beschouwd als een financieel contract en moeten ze als dusdanig aan het CAP worden meegedeeld.

In het geval effectenrekeningen het bijzondere kenmerk vertonen dat hieraan een cashpositie is verbonden, zodat met deze effectenrekening interbancaire betalingen kunnen gebeuren valt het luik cashpositie wel onder de definitie van een bankrekening en moet dit derhalve aan de hand van het IBAN-nummer aan het CAP worden gerapporteerd. Het luik echte strikte effectenrekening moet als financieel contract blijkbaar aan het CAP worden meegedeeld. Kan de minister deze interpretatie bevestigen?

Verder stelt de spreker zich de vraag of de pensioenspaarrekening onder het CAP valt. Indien de pensioenrekening rechtstreeks gecrediteerd kan worden vanuit een bankrekening, dan valt ze onder de definitie van een bankrekening.

Indien er een effectenrekening is gekoppeld aan de pensioenspaarrekening, is deze effectenrekening een financieel contract en moet het dus aan het CAP worden meegedeeld. Indien er geen effectenrekening, maar een levensverzekering van het type tak 21, 23, 25 of 26 aan de pensioenspaarrekening wordt gekoppeld, dan moet het bestaan van deze levensverzekering niet aan het CAP worden meegedeeld, want deze contracten worden immers gesloten in het kader van de derde pijler, waardoor een vrijstelling zou gelden van de mededeling. Kan de minister deze redenering bevestigen?

Verder is er de betaalrekening. Een betaalrekening is een op naam van één of meerdere betalingsdienstgebruikers aangehouden rekening, die voor de uitvoering van betalingstransacties wordt gebruikt, zoals gedefinieerd in de wet van 11 maart 2018 betreffende het statuut van en het toezicht op de betalingsinstellingen en de e-money instellingen. Dus met betaalrekening wordt eveneens bedoeld, de rekening voor elektronisch geld, op voorwaarde dat de rekening in België wordt aangehouden.

ces possibilités, parce que les intérêts qu'ils génèrent ne sont par exemple pas directement capitalisés mais d'abord versés sur le compte courant, sont-ils bien considérés comme des comptes bancaires? Autrement dit, les comptes à terme de cette nature doivent-ils être notifiés au PCC?

Les amendements présentés par le gouvernement indiquent que le champ d'application du PCC sera étendu aux comptes-titres. Mais ces comptes-titres doivent visiblement déjà être notifiés au PCC, dès lors que ce sont des contrats financiers. Normalement, les comptes-titres ne relèvent pas de la définition de la notion de compte bancaire, mais ils sont considérés comme un contrat financier et doivent à ce titre être notifiés au PCC.

Si les comptes-titres présentent la caractéristique particulière d'être liés à une position de liquidités, de telle sorte qu'ils permettent de réaliser des paiements interbancaires, le volet "position de liquidités" relève alors de la définition de la notion de compte bancaire et doit donc être notifié au PCC via le numéro IBAN. Le volet concernant strictement le compte-titre doit manifestement être notifié au PCC au titre de contrat financier. Le ministre pourrait-il confirmer cette interprétation?

L'intervenant poursuit en demandant si les comptes épargne-pension relèvent du PCC. Si le compte épargne-pension peut être directement crédité à partir d'un compte bancaire, il relève de la définition de la notion de compte bancaire.

Si un compte-titres est lié à un compte épargne-pension, ce compte-titre constitue un contrat financier, et il doit donc être notifié au PCC. Si ce n'est pas un compte-titres mais une assurance-vie des branches 21, 23, 25 ou 26 qui est liée au compte épargne-pension, l'existence de cette assurance-vie ne doit pas être notifiée au PCC, dans la mesure où ces contrats sont en effet conclus dans le cadre du troisième pilier du régime de pension, bénéficiant d'une dispense de notification. Le ministre pourrait-il confirmer ce raisonnement?

L'intervenant évoque ensuite le compte de paiement. Un compte de paiement est un compte qui est détenu au nom d'un ou de plusieurs utilisateurs de services de paiement et qui est utilisé aux fins de l'exécution d'opérations de paiement, comme le définit la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique. Le compte de paiement comprend donc aussi les comptes de monnaie électronique, pour autant que ceux-ci soient tenus en Belgique.

Verder vraagt de heer Van Quickenborne zich af of betaalkaarten of kredietkaarten aan het CAP moeten worden gemeld. Blijkbaar moet daar een onderscheid gemaakt worden tussen enerzijds betaalkaarten waarmee producten en diensten kunnen worden gekocht bij een handelaar bijvoorbeeld tankkaarten of kaarten uitgeven voor bepaalde winkelketens en anderzijds kredietkaarten, bijvoorbeeld Mastercard, Visa en dergelijke meer.

Aan de eerste categorie, de betaalkaarten, die dus toelaten om in sommige winkels op krediet te kopen, is geen betaalrekening gekoppeld waarmee klanten geldopnames kunnen doen. Dus in de praktijk moet deze dienst worden beschouwd als een betalingsfaciliteit die onder de categorie financiële contracten valt en dus moet worden gecommuniceerd aan het CAP. De kredietkaarten zijn wel gekoppeld aan een betaalrekening en moeten dus blijkbaar wel worden meegedeeld aan het CAP. Kan de minister dit bevestigen? Vallen de kredietkaarten dus onder de scope van de datamining en money control?

Verder stelt zich de vraag wie de cliënten zijn. Blijkbaar gaat het zowel over natuurlijke personen, als over rechtspersonen. Kan de minister dat bevestigen? Blijkbaar moeten ook bankrekeningen van rechtspersonen worden meegedeeld aan het CAP. Een bankrekening die gekoppeld is aan een managementgenootschap, zou dus ook in het CAP te zien zijn. Klopt de bewering dat als men dan datamining toepast op die rekening van die managementgenootschappen, men op basis daarvan dan bijvoorbeeld controles kan doen, om te zien hoeveel er op die rekening staat? Als deze bewering juist is, betekent dit dat de fiscus op die manier kan controleren of het loon dat de manager zich uitkeert via zijn managementvennootschap in verhouding is met het vermogen waarover de managementvennootschap beschikt? Kan de minister bevestigen dat bankrekeningen van managementgenootschappen ook in het CAP zijn opgenomen en dus ook zullen worden onderworpen aan het systeem van *money control*?

De identiteit van begunstigden van een financieel contract, bijvoorbeeld een begunstigde van een verzekeringscontract, indien die persoon geen mede-contractant of contractant is, moet niet worden meegedeeld aan het CAP. In dit geval moet de overdracht van de rechten van de begunstigde naar een andere begunstigde evenmin aan het CAP worden meegedeeld.

Vervolgens gaat de spreker in op de volmachtdrager. Het feit dat iemand een volmachtdrager is, dient ook in het CAP te worden vermeld. Er zijn drie voorwaarden waaraan iemand moet voldoen om als volmachtdrager te worden gekwalificeerd:

Par ailleurs, M. Van Quickenborne se demande si les cartes de paiement ou les cartes de crédit doivent être communiquées au PCC. Une distinction semble devoir être établie entre, d'une part, les cartes de paiement permettant d'acheter des produits et services auprès d'un commerçant – par exemple les cartes carburant ou les cartes émises pour certaines chaînes de magasins – et, d'autre part, les cartes de crédit, telles que Mastercard, Visa et autres.

La première catégorie, celle des cartes de paiement grâce auxquelles le client peut acheter à crédit dans certains magasins, n'est pas liée à un compte de paiement permettant d'effectuer des retraits d'argent. En pratique, ce service doit donc être considéré comme une facilité de paiement relevant de la catégorie des contrats financiers et être communiqué au PCC. Les cartes de crédit, elles, sont bien liées à un compte de paiement et doivent donc apparemment être communiquées au PCC. Le ministre peut-il le confirmer? Les cartes de crédit relèvent-elles donc du champ d'application du *data mining* et du *money control*?

Par ailleurs, il y a lieu de se demander de quels clients il est question en l'espèce. Il semble qu'il s'agisse tant des personnes physiques que des personnes morales. Le ministre peut-il le confirmer? Il semble que les comptes bancaires des personnes morales doivent également être communiqués au PCC. Un compte bancaire lié à une société de management apparaîtrait donc aussi dans le PCC. Est-il exact que le *data mining*, s'il était appliqué à ce compte de sociétés de management, permettrait par exemple d'effectuer des contrôles pour connaître le solde de celui-ci? Si cette affirmation est correcte, le fisc serait en mesure de vérifier si le salaire que le dirigeant s'octroie au travers de sa société de management est proportionné au patrimoine dont ladite société dispose. Le ministre peut-il confirmer que les comptes bancaires des sociétés de management sont également repris dans le PCC et seront donc soumis au système de *money control*?

L'identité des bénéficiaires d'un contrat financier, par exemple le bénéficiaire d'un contrat d'assurance, si cette personne n'est pas un cocontractant ou un contractant, ne doit pas être communiquée au PCC. Dans ce cas, le transfert des droits du bénéficiaire à un autre bénéficiaire ne doit pas non plus être communiqué au PCC.

Ensuite, l'intervenant aborde la question du mandataire. Lorsqu'il y a un mandataire, celui-ci doit être mentionné dans le PCC. Trois conditions doivent être remplies pour qu'une personne puisse être qualifiée de mandataire:

— er moet sprake zijn van een volmacht;

— de volmacht moet de volmachtdrager in staat stellen om in eigen naam voor rekening van een cliënt juridische handelingen te kunnen stellen;

— de volmacht moet ter kennis gebracht zijn aan de informatieplichtige.

Zowel natuurlijke personen als rechtspersonen kunnen als volmachtdrager worden beschouwd indien zij voldoen aan de drie hoger vermelde voorwaarden.

Vervolgens staat de heer Van Quickenborne stil bij een reeks bijzondere situaties.

Een eerste bijzondere situatie is de vereenvoudigde interne rekening. Iedere vereenvoudigde interne rekening die door een kredietinstelling wordt gebruikt om een storting of een afhandeling van contanten door een toevallig cliënt vast te leggen, moet op naam van die cliënt worden ingeschreven met het oog op de mededeling aan het CAP. De regeling van bankrekeningen kan dus niet worden ontweken door te werken met een vereenvoudigde interne rekening.

Een tweede bijzondere situatie bestaat uit rekeningen die slechts op één dag actief waren. Het gaat dan bijvoorbeeld om overgangsrekeningen. Ook deze rekeningen moeten gemeld worden aan het CAP. Het gaat om gelegenheidsklanten wiens verrichtingen op een overgangsrekening worden geboekt. Die rekening moeten blijkbaar ook onder het IBAN-nummer en aan het CAP worden meegedeeld op naam van de gelegenheidsklant. Dat zijn dus de zogenaamde overgangsrekeningen die meestal slechts één dag actief zijn. Hetzelfde geldt ook voor alle rekeningen of contractuele relaties die zelfs vluchtig een geldig juridisch bestaan hebben gekend.

Een derde bijzondere situatie betreft de overdracht van een bank- of betaalrekening tussen twee personen. De overdracht van een bank- of betaalrekening tussen twee personen wordt beschouwd als de afsluiting ervan in de hoofden van de vroege houder en als een opening ervan in hoofde van de nieuwe houder. Het gaat dus om twee gebeurtenissen die ook in het CAP terug te vinden zijn en dus ook onderworpen zullen worden aan datamining en *money control*.

Dan is er de informatie over financiële verrichtingen waarbij contanten zijn betrokken. In het geval informatieplichten één of meerdere financiële verrichtingen hebben uitgevoerd in België, waardoor contanten werden gestort of afgehaald door de cliënt of voor zijn rekening, moeten zij het bestaan ervan en de datum van de verrichtingen aan het CAP melden binnen bepaalde limieten. Wat

— il doit y avoir une procuration;

— la procuration doit permettre au mandataire de poser des actes juridiques en son nom propre, pour le compte d'un client;

— l'existence de la procuration doit être portée à la connaissance du redevable d'information.

Tant les personnes physiques que les personnes morales peuvent être considérées comme mandataires si elles remplissent ces trois conditions.

M. Van Quickenborne se penche ensuite sur une série de situations particulières.

Une première situation particulière est le compte interne simplifié. Tout compte interne simplifié utilisé par un établissement de crédit pour enregistrer un versement ou un prélèvement d'espèces par un "client de passage" doit être enregistré au nom de ce client en vue de sa communication au PCC. Les règles applicables aux comptes bancaires ne peuvent donc pas être contournées en recourant à un compte interne simplifié.

Une deuxième situation particulière concerne les comptes qui n'ont été actifs qu'un seul jour. Il s'agit par exemple de comptes transitoires. Ces comptes doivent également être communiqués au PCC. Ce sont les opérations de clients occasionnels qui sont enregistrées sur un compte transitoire. Le numéro IBAN de compte et le nom du client occasionnel doivent apparemment aussi être communiqué au PCC. Ces comptes dits transitoires ne sont généralement actifs qu'un seul jour. Il en va de même pour l'ensemble des comptes ou relations contractuelles qui ont eu une existence juridique valide, même lorsque celle-ci fut de très courte durée.

Une troisième situation particulière concerne le transfert d'un compte bancaire ou d'un compte de paiement entre deux personnes. Cette opération est considérée comme une clôture du compte transféré dans le chef de l'ancien titulaire, et comme une ouverture de ce compte dans le chef du nouveau titulaire. Il s'agit donc de deux événements qui doivent également figurer dans le PCC et qui seront dès lors soumis au *data mining* et au *money control*.

L'intervenant évoque ensuite les informations relatives aux opérations financières impliquant l'utilisation d'espèces. Toute personne soumise au devoir d'information qui a réalisé une opération ou plusieurs opérations financières en Belgique impliquant le versement ou le retrait d'espèces par le client ou pour son compte, doit signaler l'existence et la date de ces opérations au PCC

zijn die fameuze drempels? Dus de omwisseling van contanten tegen contanten moet enkel aan het CAP worden meegedeeld in geval de drempel van 3000 euro wordt overschreden. In het geval het om verschillende omwisselingen gaat is de melding aan het CAP verplicht als het totaalbedrag van de omwisselingen 3000 euro of meer bedraagt.

Reischeques worden blijkbaar niet beschouwd als contanten. De uitbetaling van reischeques in contanten moet dus niet aan het CAP worden meegedeeld. Iemand die leeft op reischeques, kan dus ontsnappen aan het CAP en de money control. Dus dit is dus al een eerste achterpoortje om aan de toepassing van de money control te ontsnappen.

De heer Van Quickenborne verwijst vervolgens naar de aan- of verkoop van monetaire activa in edele metalen tegen contanten. Die moeten enkel aan het CAP worden medegedeeld als de drempel van 3000 euro overschreden werd bij de verrichting of indien het globale bedrag meer dan 3000 euro bedraagt. Dit betreft bijvoorbeeld de aankoop van goud, zilver, platina, enz. In dit verband vraagt de spreker zich af of goudstaven ook onderworpen zullen worden aan de meerwaardebelasting.

De heer Jan Jambon, vice-eersteminister en minister van Financiën en Pensioenen, belast met de Nationale Loterij en de Federale Culturele Instellingen, bevestigt dat goudstaven (ook beleggingsgoud genoemd) eronder vallen, in tegenstelling tot zilver.

De heer Vincent Van Quickenborne (Open Vld) merkt op dat de aankoop van goud in de vorm van Krugerrands of Maple Leaves voor een bedrag van meer dan 3000 euro onder het CAP zal vallen.

Andere beleggingsinstrumenten zoals de ETF's (*Exchange Traded Funds*) en trackers die de evolutie van de prijs van de edele metalen volgen zijn geen monetaire activa, maar afgeleide financiële activa die niet aan het CAP moeten worden medegedeeld. Naast de reischeques vormen zij dus een tweede achterpoortje om te ontsnappen aan het CAP.

De spreker buigt zich vervolgens op de verplichte mededeling aan het CAP van alle betalingsverrichtingen of geldovermakingen tegen afgifte of opname van contanten. De stortingen op bankrekeningen of afhalingen van de bankrekening vormen in dit opzicht een uitzondering. Stortingen van contanten door de klant zelf of door zijn volmachthouders op een spaarrekening vormen een tweede uitzondering. Worden hier gevisieerd de stortingen van ouders voor hun minderjarige kind bijvoorbeeld.

dans certaines limites. À partir de quelles limites? Les opérations de change d'espèces contre espèces ne doivent être communiquées au PCC que si ces opérations excèdent le plafond de 3000 euros. Si plusieurs opérations de change ont été réalisées, la communication au PCC est obligatoire si le montant total de ces opérations est égal ou supérieur à 3000 euros.

Les chèques de voyage ne sont apparemment pas considérés comme des espèces. L'octroi de chèques de voyage en espèces ne doit donc pas être communiqué au PCC. Une personne rémunérée en chèques de voyage peut donc échapper au PCC et à tout contrôle des flux financiers. Il s'agit dès lors d'une première solution détournée pour échapper au contrôle des flux financiers.

M. Van Quickenborne évoque ensuite l'achat et la vente d'actifs monétaires en métaux précieux contre espèces. Ces opérations ne doivent être communiquées au PCC que si elles excèdent le plafond de 3000 euros ou si le montant total est supérieur à 3000 euros. Cette règle s'applique, par exemple, à l'achat d'or, d'argent, de platine, etc. À cet égard, l'intervenant se demande si les lingots d'or seront également soumis à la taxe sur les plus-values.

M. Jan Jambon, vice-premier ministre et ministre des Finances et des Pensions, chargé de la Loterie Nationale et des Institutions culturelles fédérales, confirme que les lingots d'or (également appelés "or d'investissement") seront soumis à la taxe sur les plus-values, contrairement à l'argent.

M. Vincent Van Quickenborne (Open Vld) fait observer que l'achat d'or sous la forme de Krugerrands ou de Maple Leaves pour un montant supérieur à 3000 euros devra être communiqué au PCC.

D'autres instruments d'investissement comme les ETF (*Exchange Traded Funds*) et les trackers qui suivent l'évolution du prix des métaux précieux ne sont pas des actifs monétaires, mais des actifs financiers dérivés qui ne devront pas être communiqués au CAP. Il s'agira dès lors, parallèlement aux chèques de voyage, d'une deuxième solution détournée pour échapper au PCC.

Le membre revient ensuite sur la communication obligatoire au PCC de toutes les opérations de paiement ou des transferts de fonds contre remise ou retrait d'espèces. Les versements sur les comptes bancaires ou les retraits à partir d'un compte bancaire font figure d'exception à cet égard. Les versements d'espèces par le client lui-même ou par ses mandataires sur un compte d'épargne constituent une deuxième exception visant, par exemple, les versements effectués par des parents au profit de leurs enfants mineurs.

Tweede pakket: de financiële contracten

De spreker beklemtoont dat sinds 2022 ook het periodieke geglobaliseerde bedrag van de Takken 21, 23, 25 en 26 alsook van de beleggingsovereenkomsten in het CAP moeten staan.

Voorts preciseert de heer Van Quickenborne wat men moet verstaan onder “contractuele relatie”. De regel is dat een contractuele relatie ontstaat zodra beide partijen een voorwerp, prijs en de modaliteiten hebben afgesproken en een overeenkomst hebben getekend. Op dat moment zal de informatie dus onderworpen worden aan datamining of money control. Als een notariële akte verleden moet worden voor de totstandkoming van een contractuele relatie, dan moet de informatie pas op het moment van het verleden van de akte in kwestie aan het CAP worden medegedeeld. Dit is bijvoorbeeld het geval voor hypothecaire leningen.

Te noteren valt dat de betaling van een geleende som een onderdeel is van de uitvoering van een contractuele relatie, net zoals – in sommige gevallen – het afsluiten van een kaderovereenkomst.

Het einde van een contractuele relatie vloeit voort uit het opzeggen van het contract of uit het overlijden van de cliënt. Ook deze informatie wordt aan het CAP medegedeeld. Als iemand sterft, zal de money control dus stoppen.

De overdracht van een financieel contract tussen twee personen wordt beschouwd als de afsluiting van een nieuwe contractuele relatie. In geval van gedeeltelijke overdracht moet men kijken naar de feitelijke situatie. In principe is het echter zo dat de relatie in dit geval niet geacht wordt beëindigd te zijn.

Welke financiële contracten zitten in het CAP?

De spreker wijst erop dat de verhuur van kluizen en de levensverzekeringsovereenkomsten onder het CAP zouden vallen. Dit zou echter niet het geval zijn voor de overlijdensverzekeringen en de verzekeringen gesloten in het kader van de drie pensioenpijlers (namelijk het wettelijk pensioen, de groepsverzekeringen en het pensioensparen). Kan de minister deze informatie bevestigen?

De vierde pijler integendeel (d.w.z. de levensverzekeringsovereenkomsten Tak 21 zonder fiscaal voordeel) zou wel aan het CAP moeten worden gemeld.

De heer Van Quickenborne vraagt aan minister Jambon om te preciseren of de gemengde levensverzekeringen ook aan datamining onderworpen worden.

Deuxième paquet: contrats financiers

L'intervenant souligne que, depuis 2022, le montant globalisé périodique des branches 21, 23, 25 et 26 ainsi que des contrats d'investissement, doit également être communiqué au PCC.

M. Van Quickenborne précise ensuite ce qu'il convient d'entendre par “relation contractuelle”. La règle est qu'une relation contractuelle naît dès que deux parties conviennent d'un objet, d'un prix et des modalités, et qu'elles ont signé un contrat. Ces informations sont alors soumises au *data mining* ou au *money control*. Si un acte notarial doit être passé pour l'établissement d'une relation contractuelle, les informations ne doivent être communiquées au PCC qu'au moment où l'acte notarial est passé. C'est par exemple le cas pour les emprunts hypothécaires.

Il convient de souligner que le paiement d'une somme empruntée relève de l'exécution d'une relation contractuelle, tout comme – dans certains cas – la conclusion d'un contrat cadre.

La fin de la relation contractuelle découle de la résiliation du contrat ou du décès du client. Ces informations doivent également être communiquées au PCC. Lorsqu'un contribuable décède, le contrôle des flux financiers prend fin.

Lorsqu'un contrat financier est transféré d'une personne à une autre, ce transfert est considéré comme une nouvelle relation contractuelle. En cas de transfert partiel, il convient d'examiner la situation factuelle. En principe, dans ce cas, on considère toutefois que la relation contractuelle n'a pas pris fin.

Quels contrats de crédit trouve-t-on dans le PCC?

L'intervenant souligne que la location de coffres et les polices d'assurance-vie relèveraient du PCC. En revanche, ce ne serait pas le cas pour les assurances décès ni pour les assurances souscrites dans le cadre des trois piliers de pension (à savoir la pension légale, les assurances groupes et l'épargne-pension). Le ministre peut-il confirmer ces informations?

Le quatrième pilier, par contre, (c.-à-d. les polices d'assurances vie Branche 21 sans avantage fiscal) devrait bel et bien être inscrit dans le PCC.

M. Van Quickenborne demande au ministre Jambon de préciser si les assurances vie mixtes seront également concernées par le *data mining*.

De spreker legt vervolgens de nadruk op de effectenrekeningen. Waarom heeft de minister met zijn amendementen expliciet de effectenrekeningen toegevoegd aan het CAP (cf. artikel 95/1 tot en met 8 van het wetsontwerp 56/0963) terwijl de huidige wetgeving deze reeds als financiële contracten beschouwt?

De termijnrekeningen worden gezien als een bankrekening en zijn dus in bepaalde gevallen terug te vinden in het CAP. Dit is echter niet het geval als ze niet rechtstreeks gecrediteerd of gedebiteerd kunnen worden.

Voorts vermeldt de spreker het vierde soort contracten: de hypothecaire leningen of kredieten. De openingen van kredieten/leningen zijn ook onderworpen aan het CAP.

Het volgende punt betreft de verkoopovereenkomsten op afbetaling: dienstgoederen, lichamelijke goederen, levering van diensten met betaling via periodieke stortingen, enz. zijn allemaal terug te vinden in het CAP op één uitzondering na: de financiële contracten van minder dan 200 euro, zoals bepaald in artikel VII. 3, paragraaf 3, 1°, van het Wetboek van Economisch Recht.

Leasingovereenkomsten

De heer Van Quickenborne geeft enerzijds aan dat ook de leasingovereenkomsten onderworpen zullen worden aan money control. Hij licht anderzijds toe wat men onder “leasingovereenkomst” moet verstaan: dit zijn de overeenkomsten die beantwoorden aan het criterium vastgesteld in artikel 3:89 van het koninklijk besluit van 29 april 2019 tot uitvoering van het nieuwe Wetboek van vennootschappen en verenigingen. Het voornaamste criterium waarnaar gekeken wordt om onder het toepassingsgebied van dat artikel te vallen is dat “de contractueel te storten termijnen” die verschuldigd zijn “naast de rente en de kosten ook de integrale wedersamenstelling moeten dekken van het kapitaal dat de leasinggever in het goed heeft geïnvesteerd”.

Bij een operationele leasing, waarbij het eigendomsrecht volledig bij de maatschappij blijft, moet de cliënt van de informatieplichtige niets op zijn balans inschrijven. De spreker vraagt aan minister of hij kan bevestigen dat operationele leasing dus niet aan datamining zal onderworpen worden.

Een ander element dat ook onder het CAP valt, is de leningsovereenkomst op afbetaling, op voorwaarde dat de drempel van 200 euro overschreden is. Hetzelfde geldt voor de kredietopeningen: onder de 200 euro zullen die niet in het CAP terug te vinden zijn.

L'intervenant aborde ensuite la question des comptes-titres. Pourquoi le ministre a-t-il, par ses amendements, explicitement ajouté les comptes-titres au PCC (cf. article 95/1 à 8 du projet de loi 56/0963) alors que la législation actuelle les considère déjà comme des contrats de crédit?

Les comptes-titres sont vus comme des comptes en banque et sont donc, dans certains cas, affichés dans le PCC. Néanmoins, ce ne sera pas le cas s'ils ne peuvent pas directement être crédités ni débités.

Ensuite, l'intervenant mentionne le quatrième type de contrats: les crédits ou prêts hypothécaires. Les ouvertures de crédits/prêts sont également concernées par le PCC.

Le point suivant concerne les contrats de vente à tempérament: les biens de service, les biens corporels, les prestations de services payés par versements périodiques, etc. figurent tous dans le PCC, à une seule exception près: les contrats de crédit portant sur des montants inférieurs à 200 euros, comme mentionné à l'article VII. 3, paragraphe 3, 1°, du Code de droit économique.

Contrats de leasing

M. Van Quickenborne indique, d'une part, que les contrats de leasing seront également soumis au *money control*. D'autre part, il définit ce que l'on doit entendre par “contrats de leasing”: ce sont des contrats qui répondent au critère établi à l'article 3:89 de l'arrêté royal du 29 avril 2019 portant exécution du Code des sociétés et des associations. Le principal critère pris en compte pour relever du champ d'application de cet article est que “les redevances échelonnées dues [...] couvrent, outre les intérêts et les charges de l'opération, la reconstitution intégrale du capital investi par le donneur dans la construction”.

Dans le cadre d'un leasing opérationnel, dans lequel la société de leasing conserve l'intégralité du droit de propriété, le client du redevable d'information ne doit rien inscrire dans son bilan. L'intervenant demande au ministre s'il peut confirmer que le leasing opérationnel ne sera donc pas soumis au *data mining*.

Un autre élément qui relève aussi du PCC est le contrat de prêt à tempérament, à condition que le seuil des 200 euros soit dépassé. Le même principe s'applique aux ouvertures de crédit: en-dessous de 200 euros, elles ne figureront pas dans le PCC.

De spreker vraagt ook aan de minister om zich uit te spreken over het feit dat volgende elementen al dan niet onder het CAP vallen:

— de uitgifte van een kredietkaart zou aan datamining onderworpen worden. Klopt het?

— een kasfaciliteit op een rekening-courant. Die wordt beschouwd als een kredietopening en zou moeten worden meegedeeld, maar enkel als de cliënt een natuurlijke persoon is die hoofdzakelijk handelt met een ogenmerk dat geacht kan worden vreemd te zijn aan zijn handels-, beroeps- of ambachtelijke activiteiten.

— Andere overeenkomsten krachtens dewelke een kredietverlener geldmiddelen ter beschikking stelt van een natuurlijke persoon zouden ook in aanmerking komen voor money control. De spreker geeft hier het voorbeeld van een huurgarantie, die moet beschouwd worden als een bankrekening, waarvan het rekeningnummer aan het CAP zou moeten worden medegedeeld.

— een derdenrekening: wel of niet onderworpen aan het CAP?

De werking van het CAP in de praktijk

Om onder het CAP te vallen moet het altijd gaan om contracten afgesloten in België. Het kan dus gaan om contracten die fysiek afgesloten zijn op het Belgische grondgebied. Het hangt ervan af of het contract door een Belgische informatieplichtige is gesloten of door een buitenlandse informatieplichtige die in België, via een dochtermaatschappij, een filiaal heeft – ongeacht de nationaliteit of plaats van residentie van de cliënt. Dit betekent dus dat er in het CAP ook contracten zullen opgenomen zijn die door niet-Belgen afgesloten werden. De spreker vraagt aan de minister of die redenering klopt en hoe de datamining dan georganiseerd zal worden.

Omgekeerd zal een contract dat fysiek in het buitenland afgesloten wordt met een Belgische resident, niet aan het CAP worden gemeld. Als voorbeeld geeft de spreker de situatie van een buitenlandse resident die iets afsluit met een Belgische informatieplichtige die actief is in dat land. Deze informatie zal niet het voorwerp uitmaken van datamining.

Voor de contracten die op afstand, zonder fysieke verichting, op supranationaal niveau, worden afgesloten, is money control mogelijk. Spreker haalt het voorbeeld aan van een Belgische instelling die niet actief is in een buitenlandse staat en die vanop afstand een contract afsluit met een resident van deze staat: dit contract moet aan het CAP worden meegedeeld.

L'intervenant demande également au ministre d'indiquer si les éléments suivants relèvent ou non du PCC:

— l'émission d'une carte de crédit sera soumise au *data mining*. Est-ce correct?

— une facilité de caisse sur un compte courant. Cette facilité est considérée comme une ouverture de crédit et devrait donc être communiquée, mais uniquement si le client est une personne physique agissant essentiellement à des fins réputées étrangères à ses activités commerciales, professionnelles ou artisanales.

— les autres contrats en vertu desquels un prêteur met des fonds à disposition d'une personne physique seraient également pris en considération par la législation *money control*. L'intervenant cite ici l'exemple de la garantie locative, à considérer comme un compte en banque, dont le numéro devrait être communiqué au PCC.

— un compte-tiers: doit-il ou non figurer dans le PCC?

Fonctionnement pratique du PCC

Le PCC n'est compétent que pour les contrats conclus en Belgique. Il peut donc s'agir de contrats physiquement conclus sur le territoire belge. Ce critère dépend de la question de savoir si le contrat a été conclu par un redevable d'information belge ou par un redevable d'information étranger qui possède une succursale en Belgique par l'intermédiaire d'une filiale, indépendamment de la nationalité ou du lieu de résidence du client. Il s'en déduit que le PCC disposera également d'informations concernant des contrats conclus par des étrangers. L'intervenant demande au ministre de confirmer l'exactitude de ce raisonnement et d'indiquer comment l'exploration des données sera dès lors organisée.

À *contrario*, un contrat physiquement conclu à l'étranger avec un résident belge ne sera pas signalé au PCC. À titre illustratif, l'intervenant évoque le cas d'un résident étranger ayant conclu un contrat avec un redevable d'information belge actif dans ce pays. Ces informations ne seront pas visées par l'exploration de données.

En ce qui concerne les contrats conclus à distance, sans intervention physique, au niveau supranational, le *money control* pourra s'appliquer. L'intervenant cite l'exemple d'un établissement belge qui n'est pas actif dans un État étranger et qui conclut un contrat à distance avec un résident de cet État: ce contrat devra être communiqué au PCC.

Omgekeerd wanneer een Belgische instelling, die actief is in een buitenlandse staat, vanop afstand een contract afsluit met een resident van deze staat, wordt het contract geacht in het buitenland te zijn afgesloten en maakt het geen deel uit van *money control*.

Tenslotte meldt de heer Van Quickenborne ook dat een buitenlandse instelling die niet actief is in België sowieso geen informatieplichtige is ten opzichte van het CAP.

Contracten die slechts vluchtig hebben bestaan moeten ook ter kennis worden gebracht van het CAP. Wat betreft de voorwaardelijke verbintenissen, die moeten enkel aan het CAP worden meegedeeld wanneer de voorwaarde daadwerkelijk vervuld is.

Ook de rechtelijke ontbinding van een contract, die leidt tot het ophouden van het bestaan van het contract in kwestie, moet aan het CAP worden meegedeeld.

Indien een lening aan het CAP werd meegedeeld en achteraf als nietig wordt beschouwd (een lening afgesloten door een minderjarige bijvoorbeeld), dan moet de informatieplichtige deze informatie zelf schrappen.

De spreker komt vervolgens terug op de informatie over de bank- en betaalrekeningen in het CAP. De fiscus zal voortaan het IBAN-rekeningnummer, de openingsdatum van de rekening, de identiteit van de houder, de identiteit van de volmachtdragers en de aard van de gebeurtenis (een opening zijn of een sluiting) kunnen bekijken.

Elke wijziging moet onmiddellijk aan het CAP worden meegedeeld, om ervoor te zorgen dat de gegevens accuraat zijn. Dus ook de aard en de datum van de wijziging en ook de wijziging aangebracht aan de gegevens, zoals bijvoorbeeld een wijziging van identiteit van de medehouder, een nieuwe volmachtdrager of een volmachtdrager wiens volmacht is ingetrokken.

In geval van sluiting van een rekening, zal ook het IBAN-rekeningnummer, de datum van de buitenwerkstelling en de identiteit van de houder die deze hoedanigheid verliest door de sluiting, gekend moeten worden.

Voor de financiële contracten moeten de volgende gegevens overgemaakt worden: de aard van het financiële contract, de identiteit van de cliënt en de datum van de gebeurtenis.

Als het gaat om een financiële verrichting waarbij contenten betrokken zijn, moeten de volgende gegevens in het CAP zitten: de aard van de betrokken financiële

Par contre, si un établissement belge, actif dans un État étranger, conclut un contrat à distance avec un résident de cet État, ce contrat sera réputé avoir été conclu à l'étranger et il ne sera pas soumis au *money control*.

Enfin, M. Van Quickenborne indique encore qu'un établissement étranger non actif en Belgique ne sera en aucun cas redevable d'information à l'égard du PCC.

Les contrats éphémères devront également être communiqués au PCC. En ce qui concerne les engagements conditionnels, ils ne devront être communiqués au PCC que si la condition est effectivement remplie.

La résolution judiciaire d'un contrat, qui met fin à ce contrat, doit également être communiquée au PCC.

Si un emprunt communiqué au PCC est ensuite considéré comme nul (par exemple parce qu'il s'agit d'un emprunt contracté par un mineur), le redevable d'information doit supprimer lui-même cette information.

L'intervenant revient ensuite sur les informations relatives aux comptes bancaires et aux comptes de paiement communiqués au PCC. L'administration fiscale pourra dorénavant consulter le numéro de compte IBAN, la date d'ouverture du compte, l'identité du titulaire, l'identité des mandataires et la nature de l'événement (ouverture ou clôture).

Toute modification devra être immédiatement communiquée au PCC afin de garantir l'exactitude des données, y compris, donc, la nature et la date de la modification, ainsi que la modification apportée aux données, concernant par exemple un changement d'identité du cotitulaire, un nouveau mandataire ou un mandataire dont le mandat a été révoqué.

Si un compte est clôturé, le numéro de compte IBAN, la date de clôture et l'identité du titulaire qui perdra la qualité de titulaire lors de la clôture devront également être communiqués.

En ce qui concerne les contrats financiers, les informations suivantes devront être transmises: la nature du contrat financier, l'identité du client et la date de l'événement.

S'il s'agit d'une opération financière impliquant des espèces, les données suivantes devront être communiquées au PCC: la nature de l'opération financière visée,

verrichting, de identiteit van de cliënt, de identiteit van de natuurlijke persoon die de contanten aanbiedt en de datum van de verrichting.

En als het gaat over cliënten, volmachtdragers en andere personen zullen het rijksregisternummer, de naam, voornaam, geboortedatum, geboorteplaats en geboorteland moeten vermeld worden.

Bij rechtspersonen tenslotte moet volgende informatie terug te vinden zijn in het CAP: het inschrijvingsnummer bij de Kruispuntbank van Ondernemingen (KBO), of bij gebrek aan registratie, de volledige benaming, de eventuele rechtsvorm en het land van vestiging.

Bij vennootschappen zonder rechtspersoonlijkheid gebeurt de identificatie via de natuurlijke persoon en dus via het rijksregisternummer. Worden hier gevisseerd de maatschappen, feitelijke verenigingen en in voorkomend geval alle natuurlijke personen die samen een feitelijke vereniging vormen. Deze regel geldt voor rekeningen, maar ook voor contractuele relaties en financiële contracten.

Bij een wijziging van vennootschapsvorm, behoudt die het KBO-nummer en moet er geen informatie aan het CAP worden meegedeeld. Indien de vennootschap nog geen KBO-nummer heeft en van rechtsvorm wijzigt – waardoor hij een KBO-nummer bekomt – moet die worden meegedeeld. Zo komt de omvorming van een maatschap of een feitelijke vereniging in een van de drie vennootschapsvormen (besloten vennootschap (BV), commanditaire vennootschap (CV) of naamloze vennootschap (NV) neer op de oprichting van een vennootschap. In dat geval moet het nummer aan het CAP worden meegedeeld.

De wetgeving over de uitvoering van het CAP

De heer Van Quickenborne licht de wettelijke basis voor het CAP toe. Dat is enerzijds de wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van rekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest.

Anderzijds werden twee koninklijke besluiten genomen ter uitvoering van die wet: het koninklijk besluit van 22 april 2019 tot vaststelling van de voorwaarden waaraan de voor rekening van de informatieplichtigen jegens het centraal aanspreekpunt van rekeningen en financiële contacten tussenkomende instellingen moeten voldoen om toegang te hebben tot het Rijksregister van de natuurlijke personen en het koninklijk besluit van

l'identité du client, l'identité de la personne physique qui verse les espèces et la date de l'opération.

S'il s'agit de clients, de mandataires et d'autres personnes, il conviendra de mentionner le numéro de registre national, le nom, le prénom, la date de naissance, le lieu de naissance et le pays de naissance.

Enfin, pour les personnes morales, les informations suivantes devront avoir été communiquées au PCC: le numéro d'entreprise attribué par la Banque-Carrefour des Entreprises (BCE) ou, en l'absence d'enregistrement, la dénomination complète, la forme juridique éventuelle et le pays d'établissement.

L'identification des sociétés dépourvues de personnalité juridique sera effectuée par la personne physique, et donc à partir du numéro de registre national. Il s'agit des sociétés simples, des associations de fait et, le cas échéant, de toutes les personnes physiques qui forment ensemble une association de fait. Cette règle s'appliquera aux comptes, mais également aux relations contractuelles et aux contrats financiers.

En cas de modification de la forme de société, celle-ci conservera son numéro BCE et aucune information ne devra être communiquée au PCC. Si la société ne possède pas encore de numéro BCE et change de forme juridique – après quoi elle obtient un numéro BCE –, ce numéro devra être communiqué. Par exemple, la transformation d'une société simple ou d'une association de fait visant à lui conférer l'une des trois formes de société (société à responsabilité limitée (SRL), société en commandite (SC) ou société anonyme (SA)) équivaudra à la création d'une société. Dans ce cas, le numéro devra être communiqué au PCC.

La législation relative à la mise en œuvre du PCC

M. Van Quickenborne commente la base légale du PCC. D'une part, il s'agit de la loi du 8 juillet 2018 portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt.

D'autre part, deux arrêtés royaux ont été pris en exécution de cette loi, à savoir l'arrêté royal du 22 avril 2019 fixant les conditions auxquelles les institutions intervenant pour compte des redevables d'information au point de contact central des comptes et contrats financiers doivent satisfaire pour accéder au Registre national des personnes physiques et l'arrêté royal du 6 juin 2021 modifiant l'arrêté royal du 7 avril 2019 relatif au

6 juni 2021 tot wijziging van het koninklijk besluit van 7 april 2019 betreffende de werking van het centraal aanspreekpunt van rekeningen en financiële contracten.

In het koninklijk besluit van 2019 wordt het drempelbedrag vastgelegd van 3000 euro naar aanleiding van een advies van de Gegevensbeschermingsautoriteit om zich te focussen op grotere bedragen.

Het KB preciseert ook de modaliteiten voor de mededeling van de gegevens aan het CAP door de informatieplichtigen. De termijn voor de mededeling van deze informatie is vastgelegd op drie maanden na de datum van de gebeurtenissen. In sommige gevallen is er ook sprake van een termijn van een maand en soms van vijf werkdagen. De voorziene termijn voor de saldi en de globaliseerde bedragen is telkens de laatste dag van ieder burgerlijk jaar voor de financiële contracten, en voor andere financiële contracten, 30 juni en 31 december van ieder burgerlijk jaar.

De spreker verwijst vervolgens naar artikel 10 van het KB waarin wordt bepaald dat het toezicht van de Nationale Bank op de gegevens die meegedeeld zijn aan het CAP, beperkt blijft tot de naleving van de technische vereisten en de juistheid van het ingebouwde controlenummer in het Belgische IBAN-nummer, het identificatienummer van het Rijksregister en identificatienummer van de Kruispuntbank van Ondernemingen (KBO) en Kruispuntbank van de sociale zekerheid (KSZ). Alleen die gegevens kunnen gecorrigeerd worden door de Nationale Bank en dus niet de gegevens die door de informatieplichtigen aan het CAP worden meegedeeld. Met andere woorden, als er foute gegevens worden doorgegeven aan het CAP, is dat de verantwoordelijkheid van de betrokken informatieplichtige. Kan de minister bevestigen of dat juist is?

De informatie die aan de Nationale Bank wordt verzonden en ook de antwoorden van de Nationale Bank zouden via een rechtstreekse en beveiligde verbinding gebeuren. Aangezien er hier sprake is van gevoelige gegevens, die op termijn ook onderworpen zullen worden aan datamining, had de spreker graag van de minister gehoord ten eerste over welk soort beveiligde verbinding het gaat en of er al incidenten mee geweest zijn en ten tweede of de banken die gegevens overdragen, hun cliënten kunnen geruststellen dat dit uiterst secuur gebeurt. Er zou ook – bij wijze van uitzondering – in de mogelijkheid worden voorzien om een mail sturen naar de Nationale Bank. De heer Van Quickenborne zou graag willen weten of dat effectief gebeurt en indien ja, wat de uitzonderingen precies inhouden.

fonctionnement du point de contact central des comptes et contrats financiers.

Dans l'arrêté royal de 2019, le seuil s'élevant à 3000 euros a été fixé à la suite d'un avis de l'Autorité de protection des données recommandant de se concentrer sur les montants élevés.

L'arrêté royal précise également les modalités de la communication des données au PCC par les redevables d'information. Le délai de la communication de ces informations est fixé à trois mois suivant la date des événements. Dans certains cas, le délai est d'un mois, et parfois de cinq jours ouvrables. Le délai prévu pour les soldes et les montants globalisés est à chaque fois le dernier jour de chaque année civile en ce qui concerne certains contrats financiers, et le 30 juin et le 31 décembre de chaque année civile en ce qui concerne d'autres contrats de ce type.

L'intervenant renvoie ensuite à l'article 10 de l'arrêté royal qui prévoit que le contrôle exercé par la BNB sur les données communiquées au PCC se limite au respect des exigences techniques et à l'exactitude du numéro de contrôle intégré dans le numéro IBAN belge, le numéro d'identification au Registre national des personnes physiques, le numéro d'identification attribué par la Banque-carrefour de la sécurité sociale (BCSS) et le numéro d'inscription auprès de la Banque-carrefour des Entreprises (BCE). Seules ces données peuvent être corrigées par la Banque nationale. Les données communiquées par les redevables d'information au PCC ne peuvent donc pas l'être. En d'autres termes, si des données erronées sont communiquées au PCC, c'est la responsabilité du redevable d'information concerné qui est engagée. Le ministre peut-il le confirmer?

Les informations seraient transmises à la Banque nationale par le biais d'une connexion directe et sécurisée. Il en irait de même pour les réponses de la Banque nationale. Dès lors qu'il s'agit en l'espèce de données sensibles, qui seront à terme également soumises au *data mining*, l'intervenant aurait souhaité que le ministre lui indique, premièrement, de quel type de connexion sécurisée il s'agit et si des incidents se sont déjà produits à cet égard et, deuxièmement, si les banques qui transmettent ces données peuvent rassurer leurs clients quant au fait que le processus est extrêmement sécurisé. La possibilité serait également prévue, à titre exceptionnel, d'envoyer un e-mail à la Banque nationale. M. Van Quickenborne souhaiterait savoir s'il est fait usage de cette possibilité et, dans l'affirmative, en quoi consistent exactement les exceptions.

Artikel 18 van het KB stelt dat elke persoon inzage krijgt in de gegevens die op zijn naam zijn geregistreerd, alsook op uitdrukkelijk verzoek in de lijst van de instellingen die zes maanden ervoor die gegevens hebben gecontroleerd. Dit moet dus proactief door de persoon zelf gebeuren en dat kan niet gezien worden in het systeem. De spreker richt zich tot de minister om te weten of hij van plan is om dat te wijzigen.

Als een informatieplichtige een schriftelijke aanvraag doet bij de Nationale Bank moet hij, volgens het KB, een duidelijk leesbare fotokopie recto verso toevoegen van zijn identiteitskaart en van de verblijfsvergunning die hij heeft in ons land. Voor de spreker lijkt dit een Kafkaïaans systeem te zijn.

Artikel 19 van het KB bepaalt dat elke persoon, kosteloos, in eigen persoon of door toedoen van een gevolmachtigde, de rechtzetting kan vragen van onjuiste gegevens die op zijn naam in het CAP zijn geregistreerd, hetzij aan de Nationale Bank, hetzij bij voorkeur aan de informatieplichtige die deze gegevens aan het CAP heeft meegedeeld. Graag had de spreker van de minister geweten of dit vaak voorkomt.

Tenslotte, wat de bewaartermijn betreft, is er sprake van een termijn van 10 jaar in het CAP terwijl de minister in zijn amendement naar een termijn van één jaar verwijst. Hier is de vraag hoe beide jaartallen zich ten opzichte van elkaar verhouden.

De spreker buigt zich vervolgens over de wetgeving m.b.t. datamining. De wetgeving over de bescherming van de persoonlijke levenssfeer is in dit verband relevant, meer bepaald de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (die de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens vervangt) en ook de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

De wet van 2018 voert de zogenaamde “GDPR” (*General Data Protection Regulation*) in en bevat ook specifieke bepalingen in verband met de verwerking van persoonsgegevens door overheden.

De spreker wijst erop dat artikel 5 van die wet bijzonder interessant is in het kader van de bespreking van de amendementen van minister Jambon. Dit artikel bepaalt immers dat de verwerking enkel toegestaan is als ze noodzakelijk is voor een wettelijke taak van algemeen belang. Het gaat dus over de verwerking van persoonsgegevens en het CAP valt uiteraard onder die uitzondering.

L'article 18 de l'arrêté royal prévoit que toute personne prend connaissance des données enregistrées à son nom ainsi que, sur demande explicite, de la liste des organismes qui ont contrôlé ces données au cours des six mois précédents. La personne elle-même doit dès lors agir de manière proactive, sans que cela soit visible dans le système. L'intervenant demande au ministre s'il a l'intention de modifier ce point.

Si un redevable d'information adresse une demande écrite à la Banque nationale, ce dernier est tenu, conformément à l'arrêté royal, de joindre une photocopie recto-verso bien lisible de sa carte d'identité et du titre de séjour que notre pays lui a délivré. Pour l'intervenant, ce système semble kafkaïen.

L'article 19 de l'arrêté royal prévoit que toute personne peut sans frais, en personne ou par l'intermédiaire d'un mandataire, demander la rectification de données inexactes enregistrées à son nom dans le PCC, soit à la BNB, soit de préférence auprès du redevable d'information qui a communiqué ces données au PCC. L'intervenant demande au ministre si c'est fréquemment le cas.

Enfin, en ce qui concerne le délai de conservation, il est question d'un délai de 10 ans dans le PCC, tandis que, dans son amendement, le ministre renvoie à un délai d'un an. À ce propos, la question se pose de savoir comment s'articulent ces deux chiffres.

L'intervenant évoque ensuite la législation relative au *data mining*. La législation sur la protection de la vie privée s'applique à cette matière, plus précisément la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (qui remplace la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel).

La loi de 2018 a introduit le fameux “RGPD” (Règlement général sur la protection des données) et contient des dispositions visant spécifiquement le traitement de données à caractère personnel par les autorités publiques.

L'intervenant indique que l'article 5 de cette loi est particulièrement intéressant dans le cadre de l'examen des amendements présentés par le ministre Jambon. En effet, en vertu de cet article, le traitement de données à caractère personnel n'est autorisé que s'il est nécessaire pour l'accomplissement d'une mission légale d'intérêt général. Cette exception concerne naturellement le PCC.

Rol van de Gegevensbeschermingsautoriteit ten aanzien van het CAP

De heer Van Quickenborne onderstreept dat de GBA controle uitoefent op het CAP via adviezen. De GBA zou er 6 hebben uitgebracht over het CAP.

Een van die adviezen werd al behandeld in het kader van de bespreking van de amendementen van minister Jambon. De vijf andere adviezen betreffen het advies nr. 122 van 2020, het advies nr. 14 van 2021, het advies nr. 80 van 2021, het advies nr. 203 van het jaar 2022 en het advies nr. 231 van 2022. De spreker beklemtoont dat vooral het advies nr. 122 van 2020 (advies over de wet die de saldi voorziet in het CAP) vrij kritisch is.

De spreker had van de minister graag geweten of de GBA in totaal vijf of zes adviezen heeft uitgebracht over het CAP.

Vóór 2020 heeft de spreker geen advies van de GBA kunnen terugvinden. Misschien kan dat verklaard worden door het feit dat er toen een andere privacyautoriteit was. Kan de minister meedelen welke die adviezen zijn geweest?

In haar adviezen toont de GBA zich kritisch ten aanzien van het CAP. In elk advies dat de spreker gelezen heeft, wijst de GBA op een strikte log-in van alle raadplegingen. Alles moet gelogd worden, zodat men iedere keer kan zien wie, wat, wanneer heeft geconsulteerd. De GBA verwijst ook naar periodieke veiligheidsaudits en naar een duidelijke beperking van de toegang tot de bevoegde diensten.

De heer Van Quickenborne geeft aan dat hij al eerder verwezen heeft naar het UBO-register en naar de databank van de Veiligheid van de Staat (VSSE). Via de applicatie e-Health zou het ook mogelijk zijn om te zien wie uw gegevens heeft geconsulteerd met betrekking tot de gezondheid. De GBA heeft aanbevolen dat in het kader van het CAP de burger ook inzicht krijgt in wie zijn gegevens heeft geraadpleegd. Deze aanbeveling werd nog niet uitgevoerd, maar zou door de regering bestudeerd zijn. De spreker had van minister Jambon graag preciseringen gekregen over de stand van zaken dienaangaande.

4. Vergadering van 12 november 2025

De heer Van Quickenborne (Open-Vld) begint zijn uiteenzetting met een verwijzing naar de verklaring van de eerste minister in de plenaire zitting van donderdag 6 november die verband houdt met het wetsontwerp dat besproken wordt. De eerste minister zei het volgende: "Bovendien zijn een aantal socio-economische

Rôle de l'Autorité de protection des données à l'égard du PCC

M. Van Quickenborne indique que l'APD exerce un contrôle sur le PCC au travers de ses avis. L'APD aurait rendu six avis sur le PCC.

L'un d'eux a déjà été examiné lors de la discussion des amendements présentés par le ministre Jambon. Les cinq autres sont les avis n° 122 de 2020, n° 14 de 2021, n° 80 de 2021, n° 203 de 2022 et n° 231 de 2022. L'intervenant souligne que l'avis n° 122 de 2020 (sur la loi imposant la communication des soldes au PCC) est particulièrement critique.

L'intervenant demande au ministre si, au total, l'APD a formulé cinq ou six avis au sujet du PCC.

Il n'a retrouvé aucun avis de l'APD antérieur à 2020, mais c'est peut-être dû au fait qu'une autre autorité de protection de la vie privée était compétente durant cette période. Le ministre peut-il indiquer quels furent ces avis?

Dans ses avis, l'APD est critique à l'égard du PCC. Dans tous les avis que l'intervenant a lus, l'APD insiste sur la nécessité d'enregistrer scrupuleusement toutes les consultations dans un journal pour pouvoir savoir à tout moment qui a consulté quoi et quand. L'APD mentionne aussi des audits de sécurité périodiques et une limitation claire de l'accès aux services compétents.

Outre le registre UBO et la banque de données de la Sûreté de l'État que M. Van Quickenborne a déjà mentionnés, l'application e-Health permettrait aussi à ses utilisateurs de savoir qui a consulté leurs données de santé. L'APD a recommandé que le citoyen puisse aussi savoir qui a consulté ses données au PCC. Cette recommandation n'a pas encore été mise en œuvre, mais elle aurait été étudiée par le gouvernement. L'intervenant souhaiterait que le ministre Jambon précise l'état d'avancement de cette question.

4. Vergadering van 12 november 2025

M. Van Quickenborne (Open-Vld) entame son exposé en évoquant la déclaration faite par le premier ministre à propos du projet de loi à l'examen au cours de la séance plénière du jeudi 6 novembre. Le premier ministre a déclaré ce qui suit: "De plus, plusieurs réformes socio-économiques extrêmement importantes pour la prospérité

hervormingen die zeer belangrijk zijn voor het land nog niet goedgekeurd in tweede lezing door de regering. Bijgevolg kunnen die hervormingen momenteel niet worden voorgesteld, besproken en gestemd in het parlement”.

Rekening houdend met deze verklaring vraagt de spreker zich af of de wet tot hervorming van de personenbelasting (die een verhoging van de belastingvrije som bevat) ook deel uitmaakt van dat pakket. In het kader van de bespreking van dit wetsontwerp (wet diverse bepalingen) had minister Jambon erop gewezen dat o.a. de woontaks, echtscheidingstaks, giftentaks waarvoor een belastingverlaging zou gelden via een verhoging van de belastingvrije opgenomen zouden zijn in de wet tot hervorming van de personenbelasting. Komt het wetsontwerp tot hervorming van de personenbelasting er dus nog of is dat een onderdeel van het Zomerakkoord dat niet meer besproken zal worden in dit Parlement tegen het einde van het jaar? Als de wet diverse bepalingen gestemd wordt zonder dat – daarnaast – die hervorming er komt, dan zal dat voor de mensen enkel belastingverhogingen betekenen.

De heer Van Quickenborne kaart vervolgens de problematiek van de *money control* aan. Op de ITAA-conferentie (*Institute for Tax Advisors and Accountants*) van begin november 2025 waar de commissie Financiën vertegenwoordigd was door mevrouw Alexia Bertrand (Open Vld) en waar collega's van de meerderheid en van de oppositie ook aanwezig waren, werd er ook over het CAP gesproken. Bij de oppositie is er meer enthousiasme voor het CAP dan bij de meerderheid: Vooruit was afwezig op die conferentie, mevrouw Charlotte Verkeyn (VB) zei geen andere keuze te hebben dan dit steunen en alleen de heer Dieter Vanbesien (Ecolo-Groen) was er voor. De vraag is dus of er zo weinig aandacht is voor het probleem dat de regering dit sluiks via amendementen probeert te doen opnemen in de wetgeving.

Er is blijkbaar toch persaandacht voor deze kwestie. Het tijdschrift *Moustique Magazine* heeft immers een artikel gewijd aan het gebruik van de AI door de fiscus. In het artikel “*Fliqués par les robots*” legt journalist Thomas De Picker uit hoe de fiscus overweegt om algoritmes te gebruiken om zicht te krijgen op onze bankrekeningen. Minister Jambon zou, volgens dat artikel, de artificiële intelligentie willen gebruiken om de belastingadministratie te verwittigen in geval van vermoeden van fraude. In dit opzicht wijst een bepaling in het advies van de Gegevensbeschermingsautoriteit op een ernstige inmenging in de privacy. Dit heeft de

et le bien-être de tous les citoyens de ce pays n’ont pas encore été approuvées en deuxième lecture au sein du gouvernement. Par conséquent, ces réformes ne peuvent être, pour l’instant, présentées, examinées et votées au Parlement”.

Compte tenu de cette déclaration, l’intervenant se demande si la loi portant réforme de l’impôt des personnes physiques (qui prévoit un relèvement de la quotité exemptée d’impôt) fait également partie de ce train de réformes. Lors de la discussion du projet de loi à l’examen (portant des dispositions diverses), le ministre Jambon a souligné que la taxe sur le logement, la taxe sur le divorce et la taxe sur les libéralités, entre autres, pour lesquelles une réduction serait prévue au travers d’une augmentation de la quotité exemptée d’impôt, seraient incluses dans la loi portant réforme de l’impôt des personnes physiques. Ce projet de réforme de l’impôt des personnes physiques va-t-il être déposé, ou s’agit-il d’un point de l’accord de l’été qui ne pourra plus être examiné au Parlement avant la fin de l’année? Si la loi portant des dispositions diverses est votée sans que cette réforme soit adoptée parallèlement, cela se traduira seulement par des hausses d’impôt pour les contribuables.

M. Van Quickenborne aborde ensuite la problématique du *money control*. Lors de la conférence de l’ITAA (Institut des conseillers fiscaux et des experts-comptables ou *Institute for Tax Advisors and Accountants*) de début novembre 2025, où la commission des Finances était représentée par Mme Alexia Bertrand (Open Vld) et à laquelle des collègues de la majorité et de l’opposition ont assisté, il a également été question du PCC. L’opposition se montre plus enthousiaste à l’égard du PCC que la majorité. Le parti *Vooruit* n’était pas représenté à cette conférence, Mme Charlotte Verkeyn (VB) a indiqué ne pas avoir d’autre choix que de soutenir le PCC et seul M. Dieter Vanbesien (Ecolo-Groen) y était favorable. La question est donc de savoir si le problème suscite si peu d’intérêt que le gouvernement tente d’intégrer subrepticement le PCC dans la législation par la voie d’amendements.

Il apparaît toutefois que la presse s’intéresse à cette question. Le magazine *Moustique* a en effet consacré un article à l’utilisation de l’intelligence artificielle par le fisc. Dans l’article “*Fliqués par les robots*”, le journaliste Thomas De Picker explique comment le fisc envisage d’utiliser des algorithmes pour avoir accès à nos comptes bancaires. Selon cet article, le ministre Jambon souhaite utiliser l’intelligence artificielle pour informer l’administration fiscale en cas de suspicion de fraude. À cet égard, l’un des points de l’avis de l’Autorité de protection des données évoque une ingérence grave dans la vie privée. Le ministre n’a pas changé d’avis pour autant. Au sein

minister niet van mening doen veranderen, maar bij de meerderheid vreest de MR-fractie wel voor het invoeren van een soort vermogenskadaster.

Het wetsontwerp bouwt eigenlijk voort op reeds bestaande praktijken, zoals benadrukt door doctorant aan de faculteit Rechten van de Universiteit de Namur, de heer Florian Jacques die een thesis over fiscale profilering schrijft. De belastingadministratie gebruikt al sinds meer dan 20 jaar algoritmes om fiscale fraude te bestrijden. Het systeem werd geleidelijk aan uitgebreid naar de BTW waar het goede resultaten heeft opgeleverd, volgens de doctorant. Deze stelling wordt ook door de spreker bevestigd: de schade veroorzaakt door de BTW-carrousels die honderden miljoenen hebben gekost aan de schatkist is met dat systeem veel kleiner geworden.

Expert Florian Jacques preciseert ook dat 80 % van de controles door de fiscus uit een detectie door algoritmes resulteert. Hier is het echter de bedoeling van de regering om dit systeem uit te breiden naar de databank van de Nationale Bank via het Centraal Aanspreekpunt dat bankinformatie bevat over de Belgische burgers. Er kunnen dus data worden verzameld en ingevoegd in een datawarehouse om die dan aan datamining en profilering te onderwerpen. Datamining is een geheel van technieken gebaseerd op statistieken en artificiële intelligentie, maar niemand weet wat daar precies mee gebeurt. Voor de burger is het moeilijk om te weten waarom hij gecontroleerd wordt en ook moeilijk om te betwisten. Dit gebrek aan transparantie geldt ook voor academici en professionelen omdat de overheid geen enkele informatie wil bekendmaken, wat volgens de heer Florian Jacques problematisch is.

Voorts verwijst de spreker naar het standpunt van Emmanuelle de Buisseret, juridisch adviseur bij de Ligue des droits humains. Mevrouw de Buisseret onderstreept dat de wil van de regering om de rekeningen van de burgers onder de loep te nemen beschouwd kan worden als een inmenging in de privacy en gelijkgesteld kan worden met een veralgemeend toezicht.

De heer Van Quickenborne preciseert dat het systeem van *money control* inhoudt dat alle bankrekeningen in het CAP worden gestopt en dat iedereen geacht wordt een potentiële fraudeur te zijn totdat hij zijn onschuld heeft bewezen.

In *Moustique Magazine* merkt journalist Thomas De Picker op dat in 2021 de Nederlandse regering gevallen is nadat zij tientallen duizenden burgers had vervolgd op vermoeden van fraude met kinderbijslag. Dit werd gebaseerd op het resultaat van een controle-algoritme, maar nadien is gebleken dat de meeste resultaten foutpositief

de la majorité, le groupe MR craint néanmoins la mise en place d'une forme de cadastre des fortunes.

Selon M. Jacques Florian, doctorant à la faculté de droit de l'Université de Namur, qui écrit une thèse sur le profilage fiscal, le projet de loi à l'examen s'inscrit en fait dans le prolongement de pratiques déjà existantes. L'administration fiscale utilise en effet des algorithmes pour lutter contre la fraude fiscale depuis plus de vingt ans. Ce système a été progressivement étendu à la TVA, où il aurait donné de bons résultats selon M. Florian. L'intervenant confirme également cette analyse. En effet, le préjudice des carrousels à la TVA, qui ont coûté plusieurs centaines de millions au Trésor public, a été considérablement réduit grâce à ce système.

L'expert Jacques Florian précise également que 80 % des contrôles fiscaux résultent d'une détection par des algorithmes. Cependant, l'intention actuelle du gouvernement est d'étendre ce système à la banque de données de la Banque nationale par le biais du Point de contact central, qui contient des informations bancaires relatives aux citoyens belges. Des données peuvent donc être collectées et insérées dans un *datawarehouse* avant d'être soumises à un processus de *data mining* et de profilage. Le *data mining* est un ensemble de techniques basées sur les statistiques et l'intelligence artificielle, dont personne ne connaît le fonctionnement exact. Le citoyen peut difficilement savoir pourquoi il est contrôlé, et il lui est tout aussi difficile de contester le contrôle. Ce manque de transparence s'applique aussi aux universitaires et aux professionnels, car les pouvoirs publics ne veulent rien divulguer, ce qui est problématique, selon M. Jacques Florian.

L'intervenant renvoie ensuite à la position d'Emmanuelle de Buisseret, conseillère juridique auprès de la Ligue des droits humains. Mme de Buisseret souligne que la volonté du gouvernement d'éplucher les comptes des citoyens peut être considérée comme une ingérence dans la vie privée et assimilée à une surveillance généralisée.

M. Van Quickenborne précise que le système de *money control* implique que tous les comptes bancaires seront enregistrés dans le PCC et que tout le monde sera considéré comme un fraudeur potentiel jusqu'à preuve du contraire.

Dans le magazine *Moustique*, le journaliste Thomas De Picker explique qu'en 2021, le gouvernement néerlandais est tombé après avoir poursuivi des dizaines de milliers de citoyens pour fraude présumée aux allocations familiales. Cette décision était basée sur les résultats d'un algorithme de contrôle, mais il s'est avéré par la suite

waren. De slachtoffers, hoofdzakelijk gezinnen met een migratieachtergrond, waren ondertussen hun geld kwijt en meer dan 1.100 kinderen werden aan hun ouders onttrokken. Voor de Franstaligen die meer gericht zijn op Frankrijk lijkt de situatie in Nederland misschien ver van hun bedshow, maar dat was de schandalige realiteit boven de Moerdijk. Het Syri-model – dat toegelicht zal worden door de spreker – heeft ermee te maken.

Emmanuelle de Buisseret van de Ligue des droits humains herinnert eraan dat het percentage van de bewezen fraudegevallen altijd lager is dan 1 % van alle ontvangen signalen, wat lijkt te suggereren dat de algoritmes door hun discriminerend effect meer schade veroorzaken dan ze toelaten om fraude op te sporen.

In het artikel verschenen in Moustique Magazine maakt de journalist ook gewaag van doktercontrole. Daarmee bedoelt hij het plan van de regering om datamining te gebruiken om de jacht op artsen die te veel doktersbrieven voorschrijven, te organiseren. Minister Jambon en zijn *money control* zou dus als inspiratiebron dienen voor de controle op de artsen die zich zullen moeten verantwoorden op hun voorschrijfgedrag. Volgens de heer Van Quickenborne is controle dus het mantra van deze regering.

Tot slot herneemt de heer Van Quickenborne de conclusie van de journalist. Wat betreft het gebruik van de AI weten sommige beleidsmakers waarover het gaat. Anderen zijn echter enkel uit op de resultaten en beseffen niet wat op het spel staat. Het is nochtans belangrijk om de uitdagingen goed te begrijpen want een zwak wettelijk kader zou immers door het Grondwettelijk Hof kunnen worden vernietigd en schade veroorzaken zoals in Nederland. Dit wetsontwerp is dus niet zonder gevaar voor de privacy.

De spreker komt vervolgens terug op zijn vraag om een hoorzitting met het CAP te organiseren. Die zou op 20 januari 2026 moeten plaatsvinden – als er tegen dan nog een regering is. Hij zou ook een hoorzitting willen plannen met doctorant Florian Jacques die deze materie blijkbaar goed kent. De aandacht van de pers voor deze problematiek bewijst dat er ook in Wallonië interesse is voor het respect van de persoonlijke levenssfeer.

De spreker komt nadien terug op de 6 adviezen van de Gegevensbeschermingsautoriteit (GBA) m.b.t. *money control* – één daarvan heeft betrekking op de amendementen die hier besproken worden en werd al overgemaakt; de vijf andere betreffen het advies 122 van 2020, 14 van 2021, 80 van 2021 en 203 en 231 van 2022 – en op zijn vraag om te weten of er nog andere adviezen bestaan over deze problematiek.

que la plupart des résultats étaient des faux positifs. Les victimes, principalement des ménages issus de l'immigration, avaient entre-temps perdu leur allocation et plus de 1.100 enfants avaient été retirés à leurs parents. Pour les francophones dont les yeux sont davantage tournés vers la France, la situation aux Pays-Bas peut sembler éloignée de leur réalité, mais il est important de parler de ce scandale. Le modèle SyRi – qui sera commenté par l'intervenant – y est étroitement lié.

Mme Emmanuelle de Buisseret, de la Ligue des droits humains, rappelle que le pourcentage de cas de fraude avérés est toujours inférieur à 1 % de l'ensemble des alertes reçues, ce qui semble suggérer que les algorithmes, par leur effet discriminatoire, causent plus de tort qu'ils ne permettent de détecter de fraudes.

Dans l'article paru dans Moustique, le journaliste évoque également le contrôle des médecins. Il fait référence au projet du gouvernement d'utiliser le *data mining* pour faire la chasse aux médecins qui prescrivent trop de certificats médicaux. Le ministre Jambon et son *money control* serviraient donc de source d'inspiration pour contrôler les médecins qui devront rendre des comptes sur leur comportement en matière de prescription. Selon M. Van Quickenborne, le contrôle est donc le mantra de ce gouvernement.

Enfin, M. Van Quickenborne reprend la conclusion du journaliste. En ce qui concerne l'utilisation de l'IA, certains décideurs politiques savent de quoi il en retourne. D'autres, en revanche, ne s'intéressent qu'aux résultats et n'ont pas conscience des enjeux. Il importe pourtant de bien comprendre les défis à relever, car un cadre légal faible pourrait être invalidé par la Cour constitutionnelle et causer des dommages, comme aux Pays-Bas. Le projet de loi à l'examen n'est donc pas sans danger pour la vie privée.

L'intervenant revient ensuite sur sa demande d'organiser une audition sur le PCC. Celle-ci devrait avoir lieu le 20 janvier 2026, s'il y a encore un gouvernement d'ici là. Il souhaiterait également entendre M. Florian Jacques, qui connaît bien le sujet. L'attention portée par la presse à cette problématique prouve que le respect de la vie privée suscite également de l'intérêt en Wallonie.

L'intervenant revient ensuite sur les six avis de l'Autorité de protection des données (APD) concernant le *money control*. L'un de ces avis porte sur les amendements à l'examen et a déjà été transmis. Les cinq autres sont les avis n° 122 de 2020, n°s 14 et 80 de 2021 et n°s 203 et 231 de 2022. Le membre avait également demandé s'il existait encore d'autres avis sur cette question.

Hij heeft zelf het advies 15/2018 van de Privacycommissie, de voorganger van de Gegevensbeschermingsautoriteit, over de wet van minister van Financiën Johan Van Overtveldt van 8 juli 2018 kunnen terugvinden. Hoewel het advies van de Privacycommissie zich ten opzichte van het voorontwerp van wet van minister Van Overtveldt kritisch toonde, toch was het niet zo vernietigend als het advies van de GBA over de amendementen die hier op tafel liggen. De wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van rekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest voerde een nieuw juridisch kader voor het CAP in en kwam ter vervanging van de wet van 14 april 2011 houdende diverse bepalingen die het CAP had opgericht. Oorspronkelijk was het CAP gericht op de strijd tegen fiscale fraude. In dit verband verwijst de Privacycommissie naar de relevante artikelen in het Wetboek van de inkomstenbelastingen, nl. artikel 322, § 2, waarin gepreciseerd wordt dat de toegang tot de bankgegevens door de fiscus strikt afgebakend is, en artikel 318 over het bankgeheim.

De Privacycommissie voegt eraan toe dat de gegevens bezorgd door de Nationale bank enkel gebruikt mogen worden om hetzij het bedrag van de belastbare inkomsten van de cliënt vast te stellen, hetzij de vermogenssituatie van de cliënt te bepalen met het oog op het invorderen van de belasting en de voorheffingen verschuldigd in hoofdsom en opcentiemen van de belastingverhoging en administratieve boetes van de interesten en van de kosten.

Volgens de Privacycommissie is die loutere fiscale bestemming uitgebreid geweest door de programma-wet van 1 juli 2016, met het artikel 123 dat een artikel 46 quater ingevoegd heeft in paragraaf 1 van het Wetboek van strafvordering. Dat artikel luidt als volgt: om in de eerste lid bedoelde maatregelen mogelijk te maken kan de Procureur des Konings, in geval van misdrijf bedoeld in de artikelen van de wet van 11 januari 1993 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme, “op specifiek en met redenen omkleed verzoek informatie opvragen die is opgenomen in het centraal aanspreekpunt gehouden door de Nationale Bank”. Met andere woorden kreeg het Parket in geval van witwassen ook toegang tot het CAP. De motivering was dat het CAP, gelet op zijn louter fiscale karakter, op dat moment weinig interessante informatie bood aan de personen en instellingen gemachtigd waren om informatie op te vragen bij het CAP, namelijk de Procureur des Konings, de onderzoeksrechters, de hoven- en rechtbanken inzake strafzaken, de Cel voor financiële informatieverwerking (CFI) en de notarissen optredens in

Il a lui-même retrouvé l’avis 15/2018 de la Commission de la protection de la vie privée, qui a précédé l’Autorité de protection des données, au sujet de la loi du 8 juillet 2018 du ministre des Finances, Johan Van Overtveldt. Bien que l’avis de la Commission fût critique à l’encontre de l’avant-projet de loi du ministre Van Overtveldt, il n’était pas aussi assassin que l’avis de l’APD sur les amendements à l’examen. La loi du 8 juillet 2018 portant organisation d’un point de contact central des comptes et contrats financiers et portant extension de l’accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt a instauré un nouveau cadre juridique pour le PCC, en remplacement de la loi du 14 avril 2011 portant des dispositions diverses qui avait créé le PCC. Initialement, le PCC avait pour but de lutter contre la fraude fiscale. À cet égard, la Commission de la protection de la vie privée renvoie aux articles pertinents du Code des impôts sur les revenus, à savoir l’article 322, § 2, qui précise que l’accès aux données bancaires accordé à l’administration fiscale est strictement délimité, et l’article 318 relatif au secret bancaire.

La Commission de la protection de la vie privée ajoute que les données fournies par la Banque nationale ne peuvent être utilisées que, soit pour déterminer le montant des revenus imposables du client, soit en vue d’établir la situation patrimoniale du client pour assurer le recouvrement des impôts et des précomptes dus en principal et additionnels, des accroissements d’impôts et des amendes administratives, des intérêts et des frais.

Selon la Commission de la protection de la vie privée, cette vocation purement fiscale a été étendue par la loi-programme du 1^{er} juillet 2016, par le biais de son article 123 complétant l’article 46 quater, § 1^{er}, du Code d’instruction criminelle par un alinéa rédigé comme suit: afin de permettre les mesures visées à l’alinéa 1^{er}, le procureur du Roi peut, en cas d’infractions aux articles de la loi du 11 janvier 1993 relative à la prévention de l’utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, “par sollicitation spécifique et motivée, demander des informations au Point de contact central de la Banque nationale”. En d’autres termes, le parquet a aussi obtenu l’accès au PCC en cas de blanchiment. L’argument invoqué était que, du fait de son caractère purement fiscal, le PCC n’offrait alors que très peu d’informations intéressantes aux institutions et personnes qui ont été habilitées à demander des informations au PCC, à savoir les procureurs du Roi, les juges d’instruction et les cours et tribunaux statuant en matière pénale, la Cellule de traitement de l’information financière (CTIF) et les notaires agissant dans le cadre des déclarations de succession.

het raam van successieaangiften. Het was dus belangrijk om het CAP uit deze fiscale context te verwijderen en te voorzien van een specifiek wettelijk kader.

In 2018 werden dus een aantal belangrijke wijzingen aangebracht in die wetgeving: verruiming van de doeleinden van het CAP, uitbreiding van het toepassingsgebied *ratio personae* door de wijziging van de definitie van informatieplichtige, verplichting van de informatieplichtige tot verstrekking van nieuwe informatie, verhoging van de frequentie waarmee deze informatie moet worden meegedeeld, wijziging van de nadere regels voor de gegevensoverdracht en toename van de sancties tegen de informatieplichtige in geval van niet-mededeling van de gegevens aan het CAP. De Privacycommissie heeft al die wijzigingen punt voor punt aan de privacywetgeving getoetst.

In haar negatief advies 15/2018 herneemt de Privacycommissie een tiental punten van kritiek op het voorontwerp van wet houdende organisatie van een centraal aanspreekpunt van bankrekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest van minister van Financiën Van Overtveldt.

Minister Van Overtveldt heeft zich ernaar geschikt door de wetgeving op al die punten aan te passen.

De spreker overloopt vervolgens die punten:

— in zijn eerste punt van advies onderstreepte de Privacycommissie dat het essentieel is om de rol en verantwoordelijkheden van het CAP, de informatieplichtigen en de informatiegerechtigden te preciseren;

— ten tweede moesten de doeleinden waarvoor het CAP werd ingericht, rekening houdend met de verregaande gevolgen op het privéleven, ook verduidelijkt worden. De wettelijke grondslagen moeten worden gepreciseerd;

— ten derde wees de Privacycommissie erop dat artikel 8 van het voorontwerp van wet houdende organisatie van een Centraal aanspreekpunt van bankrekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest de exclusieve verantwoordelijkheid bij de informatiegerechtigden legt. Dit om te verzekeren dat: “eenieder die namens haar een aanvraag om informatie bij het CAP indient, wordt geïdentificeerd en gelegitimeerd

Il importait donc d'extraire le PCC de ce contexte fiscal et de le doter d'un cadre légal organique spécifique.

Une série de modifications importantes ont dès lors été apportées à cette législation en 2018: élargissement des finalités pour lesquelles le PCC a été constitué, extension du champ d'application *ratione personae* par la modification de la définition de “redevable d'information”, obligation pour les redevables d'information de fournir de nouvelles informations, augmentation de la fréquence avec laquelle ces informations doivent être communiquées, changement des modalités de transfert de l'information et accroissement des sanctions encourues par les redevables d'information en cas de défaut de communication des données au PCC. La Commission de la protection de la vie privée a examiné chacune de ces modifications au regard de la législation relative à la protection de la vie privée.

Dans son avis négatif 15/2018, la Commission de la protection de la vie privée reproduit une dizaine de critiques formulées à l'égard de l'avant-projet de loi portant organisation d'un point de contact central des comptes bancaires et contrats financiers et portant extension de l'accès du fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt de M. Van Overtveldt, ministre des Finances de l'époque.

Le ministre Van Overtveldt y avait donné suite en modifiant la législation sur l'ensemble des points concernés.

L'intervenant passe ensuite ceux-ci en revue:

— dans le premier point de son avis, la Commission de la protection de la vie privée soulignait qu'il était essentiel de préciser le rôle et les responsabilités du PCC, des redevables d'information et des demandeurs d'information;

— deuxièmement, la Commission soulignait qu'il convenait aussi de préciser les finalités pour lesquelles le PCC avait été mis en place, au vu de ses conséquences importantes sur la vie privée, ainsi que ses bases légales;

— troisièmement, la Commission indiquait que l'article 8 de l'avant-projet de loi portant organisation d'un point de contact central des comptes bancaires et contrats financiers et portant extension de l'accès du fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt faisait peser sur les personnes habilitées à recevoir l'information la responsabilité exclusive de s'assurer que: “quiconque introduit une demande d'information auprès du PCC en son nom est identifié et légitime avant qu'il puisse obtenir

vooraleer hij of zij toegang tot het CAP krijgt”, en dat “iedere namens haar bij het CAP ingediende aanvraag om informatie wettig en met redenen omkleed is en de door de wetgever bepaalde finaliteit naleeft”. In haar advies geeft de Privacycommissie aan dat het belangrijk is dat de identificatie van de informatieaanvrager gebaseerd is op stevige registratieprocedures. De Commissie eist eveneens dat de aanvrager de nodige maatregelen zou nemen om de logging te registreren teneinde de aanvragen voor toegang tot het CAP te kunnen controleren. Het CAP moet er zich regelmatig van vergewissen dat de toegangen tot de gegevens van het CAP gewettigd en gerechtvaardigd zijn.

Vandaag is de login een feit en kan men ook, mits aanvraag bij de Nationale Bank, bij het CAP, nagaan wie uw gegevens als belastingplichtige heeft gecontroleerd de voorbije zes maanden.

— Een vierde punt betrof de nodige transparantie. In haar advies vroeg de Commissie in dit verband “de invoering van de mogelijkheid voor de personen van wie de gegevens in het CAP worden geregistreerd, om kennis te nemen van alle overheden, instellingen en personen die gedurende de laatste zes maanden, hun gegevens hebben geraadpleegd of bijgewerkt, met uitzondering van de gegevens van de bestuurlijke en gerechtelijke overheden die belast zijn met de opsporing en bestrafing van misdrijven”. Deze informatie kan nu bekomen worden.

— In een vijfde punt herhaalde de Privacycommissie dat “persoonsgegevens niet verder mogen worden verwerkt op een wijze die, rekening houdend met alle relevante factoren, met name de redelijke verwachtingen van de betrokkene en met de toepassing van de wettelijke en reglementaire bepalingen, onverenigbaar is met die doeleinden”. Het was hier onder meer de bedoeling om de doeleinden aan te houden, dus wat men noemt de historische, statistische en wetenschappelijke strekking en daarover was het standpunt van de commissie dat de statistische en wetenschappelijk onderzoeken in principe en bij voorkeur aan de hand van anonieme gegevens moeten gebeuren, wat nu ook zo is.

— Het zesde punt van de Privacycommissie ging over de uitbreiding van het toepassingsgebied *ratione personae* tot andere informatieplichtingen, nl. “de in België gevestigde personen die beroepshalve verrichtingen uitvoeren voor de contante aankoop of verkoop van deviezen in baar geld of met cheques in deviezen dan wel met gebruik van een krediet- of betaalkaart”, bpost en verzekeringsondernemingen. Volgens de Privacycommissie was die uitbreiding legitiem omdat het hier gaat om de bestrijding van “het witwassen van geld

accès au PCC” et que “toute demande d’information introduite en son nom auprès du PCC est légitime et motivée et respecte la finalité définie par le législateur”. Toujours dans cet avis, la Commission faisait observer qu’il était important que l’identification du demandeur d’information se base sur des procédures d’enregistrement solides. La Commission exigeait également que le demandeur prenne les mesures nécessaires pour enregistrer les *loggings* (journalisations) afin de pouvoir contrôler les demandes d’accès au PCC, en précisant que le PCC devrait régulièrement s’assurer que les accès aux informations du PCC sont légitimes et justifiés.

Aujourd’hui, cette journalisation est un fait, ce qui permet à chaque contribuable de savoir, en introduisant une demande auprès de la Banque nationale ou du PCC, qui a contrôlé ses données au cours des six derniers mois.

— Un quatrième point concernait la transparence nécessaire à prévoir. Dans son avis, la Commission demandait à cet égard “d’instaurer [...] la possibilité pour les personnes dont les informations sont enregistrées au sein du PCC de connaître toutes les autorités, organismes et personnes qui ont, au cours des six mois écoulés, consultés ou mis à jour leurs données à l’exception des autorités administratives et judiciaires chargées de la recherche et de la répression des délits.” Ces informations peuvent désormais être obtenues.

— Dans un cinquième point, la Commission réitérait que “les données à caractère personnel ne [pouvaient] pas être traitées ultérieurement d’une manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment nt des attentes raisonnables de l’intéressé et des dispositions légales et réglementaires applicables”. L’objectif était ici notamment nt de conserver ces finalités, à savoir la portée historique, statistique et scientifique, et la position de la Commission à ce sujet était que les recherches scientifiques et statistiques devaient en principe et de préférence être effectuée à l’aide de données anonymes, ce qui est aussi le cas aujourd’hui.

— Le sixième point de la Commission concernait l’extension du champ d’application *ratione personae* à d’autres redevables d’information, à savoir “les personnes établies en Belgique qui, à titre professionnel, exécutent les opérations d’achat ou de vente au comptant de devises sous forme d’espèces ou de chèques libelles en devises ou par l’utilisation d’une carte de crédit ou de paiement”, bpost et les entreprises d’assurance. Selon la Commission, cette extension était légitime dans la mesure où elle visait à prévenir “[le] blanchiment des

en de financiering van terrorisme en beperking van het gebruik van contanten, die immers kostbare informatie bezit betreffende de transacties inzake stortingen of afhalingen van contanten”.

— Het zevende punt betrof de informatiemededeling door de informatieplichtigen, die niet langer eenmaal per jaar moest gebeuren, maar continu wat betreft de relevante evenementen in verband met bankrekening en contracten. Dus bijvoorbeeld de opening, het afsluiten, de wijziging van de titularis of de gevolmachtigde: dit zal continu moeten worden meegedeeld, zodat de in het CAP geregistreerde gegevens steeds actueel en relevant zijn.

— Het achtste punt verwees naar de raadpleging van het Rijksregisternummer. De aanbeveling van de commissie in dit verband was dat dit onrechtstreeks moest gebeuren door toedoen van een instelling zoals de vereniging zonder winstoogmerk IDENTIFIN.

— In haar negende punt van kritiek stelde de Privacycommissie in haar advies 15/2018 over de bewaartermijn dat: “overeenkomstig artikel 4, § 1, 5° van de wet op de verwerking van de persoonsgegevens de persoonsgegevens niet langer mogen worden bewaard, in een vorm die het mogelijk maakt de betrokkenen te identificeren, dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij worden verkregen of verder verwerkt”. In het voorontwerp van wet van minister Van Overtveldt van 2018 was voorzien dat de bewaringstermijn zou worden bepaald bij de verschillende informatiegerechtigden, maar volgens de Privacycommissie kwam het de wetgever toe om die termijn te bepalen en die termijn werd dus ook opgenomen in de wet.

— Het tiende punt ging over het veiligheidsprincipe, zoals vervat in artikel 16 van de wet op de verwerking van de persoonsgegevens: “Het veiligheidsprincipe bij persoonsgegevensverwerkingen verplicht iedere verantwoordelijke voor de verwerking om de passende technische en organisatorische maatregelen te nemen om de persoonsgegevens te beschermen die hij verwerkt en zich te beveiligen tegen oneigenlijk gebruik. Het toereikend karakter van deze beveiligingsmaatregelen hangt enerzijds af van de stand van de techniek en de kosten en anderzijds van de aard van de te beschermen gegevens en de potentiële risico's”. Artikel 8 van het voorontwerp van wet legde de exclusieve verantwoordelijkheid bij de informatiegerechtigden om te verzekeren dat alle bij het CAP ingediende vragen om informatie opspoorbaar zijn. Het CAP moest een precieze login van de toegang bijhouden zodat, in geval van uitoefening door de betrokkene van een recht op toegang, een

capitaux et [le] financement du terrorisme et à [limiter] l'utilisation des espèces, détiennent en effet des informations précieuses en ce qui concerne les transactions qui impliquent le versement ou le prélèvement d'espèces”.

— Le septième point concernait la transmission des informations par les redevables d'information, qui ne devait plus avoir lieu une fois par an mais de manière continue concernant les événements pertinents relatifs aux comptes bancaires et contrats. Il s'agit par exemple de l'ouverture ou de la clôture d'un compte, de la modification du titulaire ou du mandataire, des informations qui doivent être communiquées en continu de sorte que les données enregistrées dans le PCC soient toujours actualisées et pertinentes.

— Le huitième point concerne la consultation du numéro de registre national. La commission a recommandé à cet égard que cette consultation soit indirecte, par l'intermédiaire d'une institution telle que l'association sans but lucratif IDENTIFIN.

— Au neuvième point de sa critique, la Commission de la protection de la vie privée indique ce qui suit dans son avis 15/2018 concernant le délai de conservation: “conformément à l'article 4, § 1^{er}, 5°, de la LVP, les données ne peuvent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement”. L'avant-projet de loi du ministre Van Overtveldt de 2018 prévoyait que le délai de conservation serait déterminé par les personnes habilitées à recevoir l'information, mais selon la Commission de la vie privée, il incombait au législateur de fixer ce délai, qui a donc été inscrit dans la loi.

— Le dixième point porte sur le principe de sécurité, énoncé à l'article 16 de la loi relative au traitement des données à caractère personnel: “Le principe de sécurisation des traitements de données à caractère personnel impose au responsable du traitement de prendre des mesures techniques et organisationnelles adéquates pour protéger les données à caractère personnel qu'il traite et de se prémunir contre les détournements de finalité. Le caractère adéquat des mesures de sécurité dépend, d'une part, de l'état de la technique et des frais engendrés et d'autre part, de la nature des données à protéger et des risques potentiels”. L'article 8 de l'avant-projet attribuait la responsabilité exclusive aux personnes habilitées à recevoir l'information pour garantir que toutes les demandes d'information introduites au PCC soient traçables. Le PCC devait tenir un registre précis des connexions afin qu'une réponse appropriée puisse être donnée en cas d'exercice du droit d'accès

passend antwoord kon worden versterkt. Ook dit werd door de wetgever geregeld.

Behalve het punt betreffende het raadplegen van het rijksregisternummer via de vzw IDENTIFIN – waarvoor hij bevestiging vraagt aan minister Jambon of dit effectief gerealiseerd werd – benadrukt de heer Van Quickenborne dat de minister van Financiën Van Overtveldt ingegaan is op alle punten van kritiek van de Privacycommissie. Dit is echter niet het geval met dit wetsontwerp en zijn amendementen. De huidige wetgever houdt geen rekening met het advies van de Gegevensbeschermingsautoriteit hierover.

Wat is de verhouding van de Grondwet tot het Centraal Aanspreekpunt (CAP) en “*Money-control*”?

De heer Van Quickenborne schetst 5 assen om te antwoorden op die vraag. Hij somt ze eerst alle vijf op en licht deze vervolgens in detail toe.

1. *Respect van het privéleven*

Artikel 22 en 22bis gaan over het respect van het privéleven (van kinderen). De spreker haalt hier het voorbeeld aan van zijn jonge dochter die over de grondrechten van kinderen moest studeren voor school. Privacy is één van die grondrechten. De spreker merkt op dat hij haar in dat kader heeft uitgelegd dat de parlementsleden momenteel het CAP en *money control* aan het bespreken zijn, wat zou kunnen inhouden dat de fiscus ook haar bankrekening zou kunnen inkijken. Dit zou een schending van de privacy betekenen. Dit voorbeeld om te illustreren dat het recht op privacy behoorlijk ver gaat, wat een goede zaak is.

2. *Legaliteit en delegatie*

Artikel 33 van de Grondwet betreft de legaliteit en de delegatie en de eis dat alle elementen altijd bij wet worden geregeld, met de debatten die ermee verbonden zijn, en dus niet bij koninklijk besluit. De spreker merkt in dit verband op dat indien het CAP via een koninklijk besluit ingevoerd was geweest, het probleem waarschijnlijk al lang geregeld was. Door het feit dat ons land een Grondwet heeft, is een regeling via KB in dit geval gelukkig niet mogelijk.

3. *Proportionaliteit*

Het gaat hier over de geschiktheid, de noodzakelijkheid en de evenredigheid in enge zin.

par la personne visée. Ce point a également été réglé par le législateur.

À l'exception du point relatif à la consultation du numéro de registre national via l'ASBL IDENTIFIN – à propos duquel il demande d'ailleurs au ministre Jambon de confirmer sa mise en œuvre effective –, M. Van Quickenborne souligne que le ministre des Finances, M. Van Overtveldt, a répondu à toutes les critiques de la Commission de la protection de la vie privée. Ce n'est toutefois pas le cas pour ce projet de loi et ses amendements. Le législateur actuel ne tient pas compte de l'avis de l'Autorité de protection des données à ce sujet.

Quelle est la relation entre la Constitution, le Point de contact central (PCC) et le *money control*?

M. Van Quickenborne présente cinq axes de réponse à cette question. Il commence par les énumérer, puis les expose en détail.

1. *Respect de la vie privée*

Les articles 22 et 22bis portent sur le respect de la vie privée (des enfants). L'intervenant illustre ce principe en citant l'exemple de sa jeune fille, qui a dû apprendre, pour l'école, en quoi consistent les droits fondamentaux des enfants, notamment le droit à la vie privée. Il précise qu'il lui a expliqué, à cette occasion, que les parlementaires parlent actuellement du PCC et du *money control* et que ce dernier pourrait permettre au fisc de consulter également son compte bancaire, ce qui constituerait une violation de sa vie privée. Cet exemple illustre la portée considérable du droit à la vie privée, qui est une bonne chose.

2. *Légalité et délégation*

L'article 33 de la Constitution porte sur la légalité, la délégation et l'exigence que tous les éléments soient toujours fixés par la loi et débattus au Parlement, et non par arrêté royal. L'intervenant fait observer que si le PCC avait été créé par arrêté royal, le problème aurait probablement été réglé depuis longtemps. Notre pays étant doté d'une Constitution, il n'est heureusement pas possible de légiférer par arrêté royal en l'occurrence.

3. *Proportionnalité*

Ce point renvoie à l'adéquation, à la nécessité et à la proportionnalité au sens strict.

4. *Scheiding der machten en onafhankelijk toezicht*

Dat zijn de artikelen 37 en 151 van de Belgische Grondwet en de rol van de Gegevensbeschermingsautoriteit.

5. *Rechtsbescherming*

Artikel 13 van de Grondwet bevat de motiverings- en transparantiebeginselen.

Wat betreft de Grondwet en het CAP onderstreept de heer Van Quickenborne dat men zou evolueren van een passieve registratie naar een actieve, geautomatiseerde selectie met potentieel dwingende gevolgen, namelijk controle en sanctie. Als het CAP dus gebruikt wordt voor datamining en profilering zal dit een nieuwe zware constitutionele last opleggen.

Artikel 22 van de Grondwet: recht op eerbiediging van het privéleven

Dat artikel waarborgt het recht op eerbiediging van het privé en gezinsleven voor iedereen, behalve in de gevallen en onder de voorwaarden door de wet bepaald. De bepaling heeft zowel een fysieke als een informatieve dimensie. Bescherming tegen de ongeloopte inmenging in de levenssfeer en tegen de ongebreidelde verwerking van persoonsgegevens.

Artikel 22bis is er gekomen met de grondwetsherziening van 2014 en voorziet dus ook in het recht op privacy en data protection voor het kind. Het feit dat men dat expliciet voorziet voor kinderen in de Grondwet, toont hoe belangrijk het ook is.

In het kader van de toetsing van het CAP aan artikel 22, moet er eerst aan herinnerd worden dat het CAP voor elke rekeninghouder de identificatie-elementen (rekeningnummers, instelling, datum opening, sluiting, volmachten en ook de saldi) registreert. Het gaat dus om gevoelige informatiedata en om een quasi-volledige index van iemands financiële infrastructuur. De loutere registratie en het raadpleegbaar maken ervan door overheden is een inmenging in artikel 22, want het beïnvloedt de autonomie en verantwoordelijkheid van de financiële levenssfeer. Het gaat bovendien om een *ex ante*, algemene en permanente registratie, niet om gerichte casusgebonden opvraging. Om te vermijden dat dit als een inmenging wordt beschouwd (en om de toets aan artikel 22 te doorstaan) moet er cumulatief voldaan zijn aan drie voorwaarden. Ten eerste moet de legaliteit bij wet worden voorzien. Er moet dus worden voorzien in voldoende precisie en voorzienbaarheid. Ten tweede moet het gaan om een legitiem doel, zijnde het algemeen belang. Fiscaliteit, bestrijding van de criminaliteit,

4. *Séparation des pouvoirs et contrôle indépendant*

Ce point renvoie aux articles 37 et 151 de la Constitution belge et au rôle de l'Autorité de protection des données.

5. *Protection juridique*

L'article 13 de la Constitution établit les principes de motivation et de transparence.

En ce qui concerne la Constitution et le PCC, M. Van Quickenborne souligne le passage d'un enregistrement passif à une sélection active et automatisée, et susceptible d'avoir des conséquences contraignantes, telles que le contrôle et la sanction. Si le PCC est utilisé pour le *data mining* et le profilage, cela imposera une nouvelle charge constitutionnelle importante.

Article 22 de la Constitution: droit au respect de la vie privée

Cet article garantit à chacun le droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi. Cette disposition a une dimension aussi bien physique qu'informatique. Elle prévoit une protection contre l'ingérence illicite dans la vie privée et contre le traitement débridé des données à caractère personnel.

L'article 22bis, inséré lors de la révision de la Constitution de 2014, prévoit donc également le droit au respect de la vie privée et la protection des données des enfants. Le fait que la Constitution prévoit explicitement cette protection pour les enfants illustre son importance.

Dans le cadre du contrôle constitutionnel du PCC au regard de l'article 22, il convient d'abord de rappeler que le PCC enregistre les données d'identification (numéros de compte, établissement, date d'ouverture, date de fermeture, procurations et soldes) de chaque titulaire de compte. Le PCC rassemble donc des informations sensibles et présente un relevé quasi exhaustif des données financières de chacun. Le simple fait d'enregistrer ces données et de permettre leur consultation par certaines autorités constitue une violation de l'article 22 en raison des conséquences sur l'autonomie et la responsabilité de la vie privée financière. Qui plus est, le projet prévoit un enregistrement *ex ante*, général et permanent, et non la possibilité d'effectuer une consultation ciblée dans le cadre d'un dossier précis. Pour éviter que les mesures à l'examen soient considérées comme une ingérence (et pour résister à l'épreuve du contrôle au regard de l'article 22), il convient de réunir trois conditions. Premièrement, la légalité devra être prévue par la loi. Celle-ci devra donc être suffisamment précise et

witwassen, kunnen die lading dekken. Ten derde moet het proportioneel zijn.

Samengevat: geschiktheid – noodzakelijkheid en evenredigheid in enge zin, met voldoende waarborgen tegen willekeur.

Heel concreet: er moeten dus controle, login, kennisgeving, kenbaarheid en ook remedies zijn.

Dit zijn de voorwaarden om in overeenstemming te zijn met artikel 22, maar niet alleen in het kader van het CAP. Die wetgeving bestond immers al en het Grondwettelijk Hof heeft daarover al een arrest geveld in 2022, waarbij het geoordeeld heeft dat het CAP grondwettig was. De toetsing aan artikel 22 moet echter niet enkel voor het CAP gebeuren, maar ook voor *money control*. En de vraag die zich hier stelt is of *money control* aan de principes van legaliteit, legitiem doel en proportionaliteit voldoet.

Artikel 33 van de Grondwet: legaliteitsvereiste

Artikel 33 van de Grondwet vergt dat de uitoefening van macht gebeurt zoals bepaald in de Grondwet. Dit impliceert dat essentiële elementen van een grondrechtenbeperking door de wetgever zelf moeten worden vastgelegd. Delegatie aan de Koning is slechts toelaatbaar voor technische modaliteiten.

De spreker onderstreept dat hij de amendementen van minister Jambon goed gelezen heeft en dat die in geen enkel koninklijk besluit voorzien. Als het gaat om databanken met gevoelige persoonsgegevens en kwesties van wie wat mag, wanneer, waarom en hoelang, dan zijn dat geen technische modaliteiten, maar wel punten die voldoende precies moeten worden geformuleerd in de wetgeving. Bijvoorbeeld het punt over de ernstige en georganiseerde fraude: in de verantwoording zegt de minister dat het daartoe beperkt is, maar die beperking is niet terug te vinden in de wetgeving. Hetzelfde geldt bijvoorbeeld voor de kwestie van wie toegang heeft tot het CAP, wie de verwerking doet. De minister zegt dat het moet gaan om adviseurs. Ook die precisering is niet terug te vinden in de wetgeving.

De wet van 2018 bevat de structuur van het CAP en somt de doeleinden en categorieën op, maar een aantal

prévisible. Deuxièmement, les mesures devront avoir une finalité légitime, à savoir servir l'intérêt public. La fiscalité ainsi que la lutte contre la criminalité et le blanchiment pourront en faire partie. Troisièmement, les mesures prévues devront être proportionnelles.

En résumé: adéquation – nécessité et proportionnalité au sens strict, avec des garanties suffisantes contre l'arbitraire.

Très concrètement: il convient de prévoir des contrôles, une journalisation, une procédure de notification, une certaine transparence et des mécanismes permettant de rectifier le tir.

Ces conditions sont nécessaires pour garantir la conformité avec l'article 22, mais pas seulement dans le cadre du PCC. Cette législation existant déjà, la Cour constitutionnelle a déjà rendu un arrêt à cet égard en 2022, dans lequel elle a estimé que le PCC respectait la Constitution. Le contrôle constitutionnel au regard de l'article 22 ne doit pas seulement être réalisé pour le PCC, mais aussi pour le contrôle des flux financiers. Et il convient de se demander si ce type de contrôle respecte les principes de légalité, de légitimité de la finalité et de proportionnalité.

Article 33 de la Constitution: exigence de légalité

L'article 33 de la Constitution exige que les pouvoirs soient exercés de la manière établie par la Constitution. Cela signifie que les éléments essentiels d'une restriction des droits fondamentaux doivent être prévus par le législateur lui-même. L'habilitation accordée au Roi doit se limiter à la définition de modalités techniques.

L'intervenant indique qu'il a lu attentivement les amendements du ministre Jambon et que ceux-ci ne prévoient aucun arrêté royal. Dès lors qu'il est question de banques de données contenant des données à caractère personnel sensibles et qu'il faut encore déterminer qui peut faire quoi, quand, pourquoi et pendant combien de temps, il ne s'agit pas de modalités techniques mais de points qui doivent être formulés de manière suffisamment précise dans la législation. Le membre évoque l'exemple de la fraude grave et organisée. Le ministre indique dans la justification que les mesures visées ne cibleront que ce type de fraude, mais cette limitation ne figure pas dans la loi en projet. Il en va de même pour les personnes qui auront accès au PCC et pour celles qui seront responsables du traitement. Le ministre a déclaré qu'il devrait s'agir de conseillers, mais la législation en projet ne le précise pas.

La loi de 2018 contient la structure du PCC et énumère les finalités et les catégories, mais elle prévoit que

aspecten werden gedelegeerd aan KB's en omzendbrieven. En, hoe algemener de wettelijke formulering, hoe groter het risico dat de essentie van de inmenging in handen komt van de uitvoerende macht. Een grondwettelijk robuust model vergt dat de wet zelf limitatief bepaalt wat de doelbinding is, de toegangsvoorwaarden, de bewaartermijnen en de kennisgevings- en remedie-regimes. Dus, een potentiële uitbreiding van het CAP naar een actieve verwerking met selectie, onderzoek en dwangbevoegdheden, kan constitutioneel niet op basis van bestaande delegaties worden gebouwd. Ze vergt een nieuwe, specifieke wet die de finaliteit, de methodologie, de technische waarborg, de menselijke tussenkomst en de rechtsmiddelen expliciet zal beschrijven.

Proportionaliteit als grondwettelijk beginsel

Dit staat niet als zodanig in de Grondwet, maar maakt deel uit van onze grondwettelijke gewoontes. Het Grondwettelijk Hof past in dit verband een driedelige evenredigheidstoets toe.

Het is een drietrapsraket. Ten eerste, de geschiktheid: draagt de maatregel rationeel bij tot het doel? Ten tweede, de noodzakelijkheid: bestaat er een minder ingrijpend alternatief dat hetzelfde doel kan bereiken? En ten derde, de evenredigheid in de enge zin: weegt het voordeel voor het algemeen belang op tegen het nadeel voor het individuele recht?

Dat zijn de drie elementen die het grondwettelijk hof consequent toetst.

De spreker past die drie toetsingselementen van het Grondwettelijk Hof op het CAP toe.

— De geschiktheid

Draagt de maatregel rationeel bij tot het doel? Ja. Centrale identificatie versnelt onderzoek en invordering. Dus de bedoeling van het CAP was om ervoor te zorgen dat in plaats van een administratieve loge procedure waarbij men dus banken moest bevragen, men via het CAP kon gaan en op die manier kon zien wie waar rekening aanhoudt om dan desgevallend de bank te bevragen.

— De noodzakelijkheid

Bestaat er een minder ingrijpend alternatief dat hetzelfde doel kan bereiken? Dat is problematisch omdat de registratie de volledige bevolking betreft

certaines modalités seront précisées par arrêté royal et par circulaire. Or, plus la formulation légale est vague, plus le risque est grand que les éléments essentiels de cette ingérence soient réglés par le pouvoir exécutif. Un modèle constitutionnellement solide requiert que la loi fixe elle-même, de manière exhaustive, la finalité, les conditions d'accès, les délais de conservation, les règles relatives à la notification et les mécanismes permettant de rectifier le tir. En conclusion, toute extension éventuelle du PCC pour permettre un traitement actif des données, qui impliquerait un processus de sélection, un examen et des pouvoirs de contrainte, n'est constitutionnellement pas possible sur la base des délégations actuellement prévues par la loi. Cette extension nécessiterait une nouvelle loi spécifique qui décrirait explicitement la finalité, la méthodologie, les garanties techniques, l'intervention humaine et les voies de recours.

La proportionnalité en tant que principe constitutionnel

La proportionnalité ne figure pas en tant que telle dans la Constitution, mais fait partie de nos habitudes constitutionnelles. La Cour constitutionnelle applique un contrôle de proportionnalité en trois parties.

Il s'agit d'un processus en trois étapes. Premièrement, l'adéquation: la mesure contribue-t-elle de manière rationnelle à l'objectif poursuivi? Deuxièmement, la nécessité: existe-t-il une alternative moins radicale permettant d'atteindre le même objectif? Et troisièmement, la proportionnalité au sens strict: l'avantage pour l'intérêt général l'emporte-t-il sur l'inconvénient pour le droit individuel?

Ce sont les trois éléments que la Cour constitutionnelle examine systématiquement.

L'intervenant applique ces trois critères de contrôle de la Cour constitutionnelle au PCC.

— L'adéquation

La mesure contribue-t-elle de manière rationnelle à l'objectif poursuivi? Oui. L'identification centrale accélère les enquêtes et les recouvrements. L'objectif du PCC était de remplacer une procédure administrative fastidieuse, qui consistait à interroger les banques, par une consultation du PCC, qui permet de savoir qui détient un compte dans quelle banque, afin de pouvoir interroger la banque, le cas échéant.

— La nécessité

Existe-t-il une alternative moins radicale permettant d'atteindre le même objectif? Ce point pose problème, car l'enregistrement concerne l'ensemble de la population,

zonder risico-indicaties. Er zijn natuurlijk alternatieven denkbaar. Bijvoorbeeld in het advies van de Gegevensbeschermingsautoriteit wordt er gepleit voor online toegang, rechtstreekse toegang tot het CAP. Wat men veel minder intrusief vindt. Je zou gefaseerde toegang kunnen voorzien op basis van concrete aanwijzingen of voorzien in een tijdelijke opslag, in plaats van een permanente centrale opslag.

— *De evenredigheid*

Weegt het voordeel voor het algemeen belang op tegen het nadeel voor het individuele recht? Dat is twijfelachtig, want de diepe impact op de financiële privacy, de permanente beschikbaarheid en het gebrek aan kennisgeving en remediemechanismen wegen zwaar, terwijl het doel niet per se algemene en permanente registratie vergt.

Dus als die drie elementen getoetst worden, dan zijn die al twijfelachtig. Maar er is ook nog het arrest van het Grondwettelijk Hof van 2022 waarin die toetsing ook gedaan werd. De heer Van Quickenborne komt daar later op terug, weliswaar met een kritische noot.

Rekening houdend met die drie principes vraagt de spreker zich af of de wetgeving wel stand houdt. Want zodra de data van het CAP voor profilering dienen, stijgt de intensiteit van inmenging en dus het risico op foutpositieven, stigmatisering en automatisering van beslissingsroutes.

De spreker vervolgt zijn uiteenzetting met het punt van de uitbreiding van het gebruik van het CAP voor profilering, waardoor er nog meer inmenging is en het nog moeilijker te verantwoorden wordt dat, zonder strikte doelaafbakening, zonder ex-ante onafhankelijke controle en zonder menselijke toets in het proces, het toch lukt.

De evenredigheid in enge zin kantelt negatief als burgers geen ex-postkennis en effectief rechtsmiddel hebben. De heer Van Quickenborne wijst minister Jambon er dus op dat hij heel grote risico's neemt met zijn amendementen op basis van de proportionaliteit. Als die zaak voor het Grondwettelijk Hof wordt gebracht – en als dat niet gebeurt dan zal de spreker het zelf doen als belanghebbende met een bankrekening in deze zaak – gaat hij ervan uit dat het resultaat deze keer (na het arrest van 2022) vernietigend zal zijn.

sans indices de risques. Des alternatives sont bien sûr envisageables. Par exemple, dans son avis, l'Autorité de protection des données plaide en faveur d'un accès direct au PCC en ligne, ce qui est considéré comme beaucoup moins intrusif. On pourrait prévoir un accès progressif sur la base d'indices concrets ou prévoir un stockage temporaire, plutôt qu'un stockage central permanent.

— *La proportionnalité*

L'avantage pour l'intérêt général l'emporte-t-il sur l'inconvénient pour le droit individuel? On peut en douter, car l'impact profond sur la vie privée financière, la disponibilité permanente et l'absence de notification et de mécanismes de recours pèsent lourdement dans la balance, alors que l'objectif ne requiert pas nécessairement un enregistrement général et permanent.

Si ces trois éléments sont examinés, ils sont donc déjà discutables. Mais l'intervenant renvoie aussi à l'arrêt de la Cour constitutionnelle de 2022, dans lequel ce contrôle a également été effectué. M. Van Quickenborne y reviendra plus tard, de manière certes critique.

Compte tenu de ces trois principes, l'intervenant se demande si la législation résistera. En effet, dès que les données du PCC seront utilisées à des fins de profilage, l'ingérence se fera plus intense, et donc le risque de faux positifs, de stigmatisation et d'automatisation des processus décisionnels augmentera lui aussi.

L'intervenant poursuit son exposé en abordant la question de l'extension de l'utilisation du PCC à des fins de profilage, ce qui accroît l'ingérence et rend encore plus difficile de justifier que le système fonctionne correctement sans délimitation stricte des objectifs, sans contrôle indépendant *ex ante* et sans contrôle humain dans le processus.

On peut considérer que la proportionnalité au sens strict n'est plus respectée lorsque les citoyens ne sont pas informés *a posteriori* et ne disposent pas de recours juridique efficace. M. Van Quickenborne attire donc l'attention du ministre Jambon sur le fait qu'il prend des risques très importants avec ses amendements fondés sur la proportionnalité. Si cette affaire est portée devant la Cour constitutionnelle – et si ce n'est pas le cas, l'intervenant le fera lui-même en tant que partie intéressée disposant d'un compte bancaire dans cette affaire –, il part du principe que le résultat sera cette fois (après l'arrêt de 2022) accablant.

— *Scheiding der machten en onafhankelijk toezicht*

De spreker beklemtoont dat deze materies in artikel 37 en 151 van de Grondwet worden geregeld. Eerst en vooral is er de concentratie van functies. De Nationale Bank beheert het CAP en de FOD Financiën, het Parket, de Cel voor financiële informatieverwerking (CFI) en anderen gebruiken het. Ze ressorteren allemaal onder de uitvoerende macht. En dus zonder externe, onafhankelijke, voorafgaande autorisatie, bijvoorbeeld van een rechter of functionele instantie met inzicht in het dossier, ontstaat machtsconcentratie. Het is dezelfde staatsmacht die registreert, selecteert en gebruikt, met slechts interne administratieve checks. En dat botst met de checks-and-balances-logica van onze Grondwet. De Gevensbeschermingsautoriteit speelt daarbij ook een rol. Die is inderdaad onafhankelijk, maar effectief toezicht vereist ook informatie- en handhavingsmacht en die is niet voorzien in onze wetgeving. Dus de GBA kan niet in beroep gaan tegen een bepaalde wetgeving. Dat was initieel voorzien in het ontwerp van meneer Mathieu Michel, maar werd onder de vorige regering door de Vooruit-fractie verworpen. De heer Van Quickenborne voegt hier ironisch aan toe dat als het over privacy gaat, Vooruit het zich niks van aan trekt. Alles wordt toch op de sociale media gepubliceerd. Hij verwijst in dit verband naar social-media socialisme waarin de privacy tot nul wordt herleid.

De heer Van Quickenborne benadrukt dat hij wel in de GBA gelooft en dat die instantie noodzakelijk is. Hij onderstreept anderzijds dat er nog parlementsleden, democraten, zijn in dit halfroond die de verschillende machten respecteren alsook de rol van de GBA.

Hij juicht ook de tussenkomst van de heer Benoît Lutgen (Les Engagés) toe, vooral wat betreft de vrijheid van vereniging en het feit dat ook op dat vlak de Grondwet nageleefd moet worden. Ook ten opzichte van dit wetsontwerp van de regering – waarbij velen eveneens vragen hebben – blijft de heer Lutgen waakzaam.

De GBA is dus onafhankelijk, heeft een advies uitgebracht, maar heeft niet de nodige handhavingsmacht om dergelijke wetgeving tegen te houden.

Tot slot stelt de heer Van Quickenborne dat het binnen het aspect onafhankelijk toezicht (artikel 151 van de Grondwet) ook aangewezen is om, bij veeleisende inmengingen in het privéleven – zeker als het gaat over profilering –, constitutioneel te voorzien in een rechtelijke voorafgaande toestemming of onafhankelijke autorisatie.

— *Séparation des pouvoirs et contrôle indépendant*

L'intervenant souligne que ces matières sont réglées par les articles 37 et 151 de la Constitution. D'abord et avant tout, il évoque la concentration de fonctions. La Banque nationale gère le PCC, tandis que le SPF Finances, le parquet, la Cellule de traitement des informations financières (CTIF) et d'autres instances l'utilisent. Tous relèvent du pouvoir exécutif. Par conséquent, sans autorisation préalable externe et indépendante, par exemple d'un juge ou d'une instance fonctionnelle ayant connaissance du dossier, on assiste à une concentration du pouvoir. C'est le même pouvoir étatique qui enregistre, sélectionne et utilise, avec seulement des contrôles administratifs internes. Et cela va à l'encontre de la logique d'équilibre des pouvoirs prévue par notre Constitution. L'Autorité de protection des données joue également un rôle à cet égard. Elle est certes indépendante, mais un contrôle efficace nécessite également un pouvoir d'information et de recours, qui n'est pas prévu dans notre législation. L'APD ne peut pas introduire un recours contre une législation donnée. Cette compétence était initialement prévue dans le projet de M. Mathieu Michel, mais a été rejetée par le groupe Vooruit sous le gouvernement précédent. M. Van Quickenborne ajoute non sans ironie que Vooruit se moque éperdument du respect de la vie privée. Tout finira de toute façon sur les réseaux sociaux. Il fait référence à cet égard au socialisme des réseaux sociaux, où la vie privée est réduite à néant.

M. Van Quickenborne souligne qu'il croit en l'APD et que cette instance est nécessaire. Il souligne d'autre part qu'il y a encore des parlementaires, des démocrates, dans cet hémicycle qui respectent les différents pouvoirs ainsi que le rôle de l'APD.

Il salue également l'intervention de M. Benoît Lutgen (Les Engagés), surtout en ce qui concerne la liberté d'association et le fait que la Constitution doit également être respectée dans ce domaine. M. Lutgen reste vigilant à l'égard de ce projet de loi du gouvernement, qui suscite également des questions de la part de nombreux autres membres.

L'APD est donc indépendante, a rendu un avis, mais ne dispose pas du pouvoir nécessaire pour contrer une telle législation.

Enfin, M. Van Quickenborne estime qu'en ce qui concerne l'aspect du contrôle indépendant (article 151 de la Constitution), il convient également, en cas d'ingérence profonde dans la vie privée – certainement en cas de profilage –, de prévoir dans la Constitution une autorisation judiciaire préalable indépendante. Une simple

Een louter administratieve toegangsdrempel volstaat niet wanneer de inmenging structureel, universeel en permanent is.

— *Het eigendomsrecht*

Het eigendomsrecht bevat niet alleen de fysieke goederen, maar ook de economische autonomie en de vertrouwelijkheid van financiële dispositie. Dus het CAP verandert de positie- evenwicht in het nadeel van de burger, want de overheid weet systematisch waar vermogen is aangehouden.

Ook als is dit geen onteigening, toch kan dat de vrijheid van vermogensbeheer en het vertrouwen aantasten.

— *Toegang tot de rechter*

Artikel 13 van de Grondwet garandeert de toegang tot de rechter, maar effectiviteit veronderstelt kennis. Stel dat een belastingplichtige wordt gehoord voor mogelijke fraude op basis van het systeem van *money control* en dat hij naar de rechter gaat en heeft geen kennisgeving, zelfs niet achteraf, van een raadpleging of een selectie, dan kan hij die schending niet aanvechten. Dus de GBA-procedure moet ook praktisch openstaan. Een burger moet zijn raadpleging nog kunnen laten verifiëren en onrechtmatig gebruik kunnen laten sanctioneren.

Er is ook het punt van de motiverende transparantie. Het beginsel van behoorlijk bestuur, motiveringsplicht, zorgvuldigheid en gelijkheid vergen dat ingrijpende verwerkingen uitlegbaar zijn. Bij profilering wordt die eis acuut. Wie geselecteerd wordt, moet kunnen weten waarom en het tegenbewijs kunnen leveren. Anders wordt de rechtsbescherming theorie. En dat is het probleem.

Het systeem van *money control* is een soort van chat control, maar over de bankrekeningen, inclusief de saldi. Als je dat in een systeem van datawarehouse zet en als alles op basis van algoritmes gebeurt, is het moeilijk om je te verdedigen voor een rechtbank omdat je niet weet waarom en hoe je werd geselecteerd. De spreker komt daar nog later op terug.

In dit verband verwijst hij ook naar een wetsvoorstel van Les Engagés, getekend door mevrouw Matz, meneer Prevot, mevrouw Fonck, meneer Dallemagne. Voor de vijfde persoon, namelijk Josy Arens, twijfelt de spreker of hij het wetsvoorstel ook meegetekend had. Het idee

barrière administrative ne suffit pas lorsque l'ingérence est structurelle, universelle et permanente.

— *Le droit à la propriété*

Le droit à la propriété ne porte pas uniquement sur les biens physiques, mais également sur l'autonomie économique et sur la confidentialité des opinions financières. Donc, le PCC modifie l'équilibre au détriment du citoyen puisque les autorités publiques savent désormais systématiquement où le patrimoine est détenu.

Certes, ce n'est pas une expropriation, mais cela peut entamer la liberté de gestion du capital et la confidentialité.

— *Accès au juge*

L'article 13 de la Constitution garantit l'accès au juge. Pour autant, l'efficacité suppose la connaissance. Imaginons qu'un contribuable soit entendu pour suspicion de fraude détectée par le système de *money control* et qu'il se rende devant le juge, mais sans avoir été informé, même *a posteriori*, que les autorités ont consulté ses données et l'ont sélectionné, il ne pourra alors pas tenter de recours contre cette violation de sa vie privée. Dès lors, la procédure devant l'APD doit également être pratiquement accessible. Un citoyen doit pouvoir faire vérifier la consultation de ses données et faire sanctionner leur utilisation abusive.

Il y a aussi la question de la transparence motivée. Au regard des principes de bonne gouvernance, d'obligation de motivation, de précaution et d'égalité, les traitements approfondis de données doivent être explicables. En cas de profilage, cette exigence est d'autant plus forte. Les contribuables sélectionnés doivent pouvoir savoir pourquoi ils l'ont été et pouvoir contester cette sélection. Faute de quoi, la protection juridique restera un simple concept théorique. C'est là que réside le problème.

Le système du *money control* s'apparente au *chat control*, mais il porte sur les comptes en banque, y compris leur solde. Si ce dispositif s'inscrit dans un système de *datawarehouse* et qu'il fonctionne entièrement sur la base d'algorithmes, il sera difficile à défendre devant un tribunal, car il est impossible, dans ce cas, pour un contribuable de savoir pourquoi et comment il a été sélectionné. L'intervenant reviendra ultérieurement sur ce point.

À cet égard, il revient également sur une proposition de loi des Engagés, signée par Mme Matz, M. Prevot, Mme Fonck et M. Dallemagne. Quant à la cinquième personne, M. Josy Arens, l'intervenant n'est pas certain qu'elle ait également signé la proposition de loi. L'idée de

van dit wetsvoorstel bestond erin om die algoritmes op te nemen in de wet op de openbaarheid van bestuur en in de Commissie voor de toegang tot bestuursdocumenten.

De heer Van Quickenborne herhaalt in het kort zijn laatste punt over de grondwettelijke bescherming en de artikelen die hij in dit verband toegelicht heeft. Hij legt ook de nadruk op de moeilijkheid om zich voor de rechter te verdedigen als je niet weet waarom je geselecteerd werd. Dit komt door die fameuze algoritmes en de DAM-fiches, waarop hij zal terugkomen en waarover hij ook een schriftelijke vraag heeft gesteld.

— Privacy voor minderjarigen

Dit wordt voorzien in artikel 22bis van de Grondwet. Het is opvallend dat de grondwetgever in 2014 een dergelijk artikel in de Grondwet heeft ingeschreven. Het ging dus niet over de vrijheid van meningsuiting of over andere fundamentele rechten, maar wel over privacy. Dit betekent volgens de spreker dat de wetgever van mening was dat er verhoogde waarborgen moesten zijn om dit recht te beschermen. Het CAP maakt geen onderscheid tussen minderjarigen en volwassenen. De rekeningen en contracten waarbij minderjarigen betrokken zijn, worden ook opgenomen in het CAP. Die verhoogde waarborgen houden dus in dat er striktere toegangsdrempels, beperktere bewaartermijnen en bijzondere kennisgevings- en remedies via ouders en voogden moeten zijn. Want profilering van gezinnen en ouders met doorwerking naar kinderen is extra gevoelig en vergt een striktere noodzaaktoets.

En dan is er de sprong naar *money control*, datamining en de geautomatiseerde selectie. Datamining voegt nieuwe verwerkingsdoeleinden toe, dus risico-inschatting. Het voorziet ook nieuwe verwerkingsmiddelen, zijnde de algoritmes en impliceert nieuwe gevolgen en verhoogde kansen op controle.

Dit is kwalitatief anders dan passief registerbeheer. Constitutioneel betekent dit dat ook hier zwaardere waarborgen zijn vereist en dat het legaliteitsniveau moet stijgen. Dat betekent een heldere wet, strikte doelbinding en een menselijke eindbeslissing.

— Grondwettelijke minimumnormen voor profilering

Welke minimumnormen zouden er moeten zijn voor profilering?

ce texte était d'intégrer ces algorithmes dans la loi relative à la publicité de l'administration et de les communiquer à la commission d'accès aux documents administratifs.

M. Van Quickenborne répète brièvement son dernier point relatif à la protection constitutionnelle et aux articles qu'il a développés en la matière. Il souligne également la difficulté pour le contribuable d'assurer sa défense devant le juge s'il ignore la raison pour laquelle il a été sélectionné. Cela s'explique par les fameux algorithmes et les fiches DAM, sur lesquels il reviendra et à propos desquels il a également posé une question écrite.

— Respect de la vie privée des mineurs d'âge

Ce droit est consacré par l'article 22bis de la Constitution. Ce choix du législateur constitutionnel d'inscrire, en 2014, un tel article dans la Constitution interpelle. Il ne s'agissait pas de la liberté d'expression ou d'un autre droit fondamental, mais bien du droit au respect de la vie privée. Aux yeux de l'intervenant, cela signifie que le législateur était d'avis que des garanties accrues étaient nécessaires afin d'assurer la protection de ce droit. Le PCC n'opère aucune forme de distinction entre les mineurs d'âge et les adultes. Les comptes et les contrats dans lesquels des mineurs sont impliqués y figurent également. Ces garanties renforcées impliquent donc des règles d'accès plus strictes, des délais de conservation plus courts et des obligations particulières de notification et des voies de recours spécifiques via les parents et les tuteurs. En effet, l'implication des enfants dans le profilage des ménages et des parents est un sujet ultrasensible qui demande le respect d'un critère strict de nécessité.

L'étape suivante est donc celle du *money control*, du *data mining* et de la sélection automatisée. Le *data mining* ajoute de nouvelles finalités de traitement, et donc l'évaluation des risques. Cette technique prévoit également de nouveaux outils de traitement, à savoir les algorithmes, et implique de nouvelles conséquences et une probabilité de contrôle accrue.

Sur le plan qualitatif, cette méthode n'a rien d'une gestion passive des registres. Il s'ensuit qu'elle requiert également des garanties constitutionnelles plus robustes et que le niveau de légalité doit augmenter. Cela doit se traduire par une loi plus claire, une finalité bien définie et une décision finale prise par un être humain.

— Normes constitutionnelles minimales pour le profilage

Quelles devraient être les normes minimales pour le profilage?

In de eerste plaats, een wettelijke basis met een limitatieve finaliteit. Dit staat niet vermeld in de amendementen van minister Jambon. Er is wel een wettelijke basis, nl. die amendementen, maar er is geen limitatieve finaliteit per doeleinde. Er is geen sprake meer van enkel fiscaliteit, witwas of straf. Het komt dus neer op een onbeperkte finaliteit, aangezien het elke overtreding die gepleegd wordt tegen een regel betreft. Hiervoor verwijst de spreker naar het voorgestelde vierde en vijfde lid van paragraaf 3 van artikel 5 van de wet van 3 augustus 2012 dat door amendement nr. 16 (DOC 56 0963/005, p. 11-20) wordt ingevoegd.

Ten tweede, een *ex ante* onafhankelijke autorisatie om zeker te zijn dat er wel degelijk onafhankelijk wordt gehandeld.

Ten derde, een menselijke tussenkomst. Minister Jambon geeft aan dat die menselijke tussenkomst er is en hij verwijst daarvoor naar bepaalde alinea's in zijn tekst. Maar de heer Van Quickenborne heeft het over een menselijke tussenkomst met verantwoordelijkheid en motivering. Als de menselijke tussenkomst enkel wat men noemt "*rubber stamping*" is, of "lettre à la poste", dan is dat geen volwaardige menselijke tussenkomst. Te noteren valt dat er in Nederland, bij de toeslagen-affaire (ook Syri-affaire genoemd) ook sprake was van een "menselijke" tussenkomst, maar de rechter heeft geoordeeld dat die zeer minimalistisch was. In de tekst van minister Jambon wordt er gepreciseerd dat bij depseudonymisatie, de controledienst zich over het dossier zal buigen. Het gebruik van de "zal" (onvoltooid tegenwoordige toekomstige tijd) in de tekst betekent dat er geen discussionaire bevoegdheid meer is voor een mens. Het zal dus automatisch gebeuren en de menselijke tussenkomst is herleid tot "*rubber stamping*".

Ten vierde, om het grondwettelijk conform te maken, moet *money control* ook in de kennisgeving achteraf voorzien. Dat is belangrijk voor de rechtelijke toets achteraf want als mensen naar de rechtbank stappen, moeten zij dat op een correcte manier kunnen doen.

Wat er ook ontbreekt in de wetgeving van de minister, is recht op uitleg, betekenisvolle informatie over de logica, recht op correctie van feitelijke onjuistheden en recht op betwisting van de uitkomst. Dat zijn allemaal zaken die niet in de zeven alinea's van de ontwerp-tekst terug te vinden zijn en die de tekst grondwettelijk zeer kwetsbaar maken. In dit verband vraagt de heer Van Quickenborne zich af of dit eigenlijk niet de ware bedoeling van minister Jambon is: misschien hoopt de minister stilletjes verlost te zijn van die *money control* bij vernietiging door het Grondwettelijk Hof en zo verlost te zijn van dat koekoeksei dat Vooruit in zijn nest heeft gelegd.

Premièremment, une base légale assortie d'une finalité limitative doit être prévue. Celle-ci ne figure pas dans les amendements du ministre Jambon. Une base légale a bien été prévue, par ces amendements, mais aucune finalité limitative par objectif. Il n'est plus seulement question de fiscalité, de blanchiment d'argent ou de sanctions. La finalité sera donc illimitée, puisqu'elle concernera toute infraction commise à l'encontre d'une règle. L'intervenant renvoie à cet égard à l'article 5, § 3, alinéas 4 et 5, de la loi du 3 août 2012 inséré par l'amendement n° 16 (DOC 56 0963/005, pages 11-20).

Deuxièmement, une autorisation *ex ante* indépendante doit être délivrée afin de garantir que l'action est bien indépendante.

Troisièmement, une intervention humaine doit être prévue. Le ministre Jambon indique que cette intervention humaine a été prévue et renvoie à cet effet à certains paragraphes de son texte. Or, M. Van Quickenborne parle d'une intervention humaine responsable et motivée. Si l'intervention humaine se limite à valider rapidement l'opération comme on met une lettre à la poste, il ne s'agira pas d'une intervention humaine à part entière. Il convient de noter que, dans l'affaire des allocations familiales (également appelée affaire Syri) aux Pays-Bas, il était également question d'une intervention "humaine", mais que le juge a conclu qu'elle était très minimaliste. Le texte du ministre Jambon précise qu'en cas de dépseudonymisation, le service de contrôle se penchera sur le dossier. L'emploi du futur simple dans le texte signifie qu'il n'y aura plus de marge de discussion pour un être humain. La procédure sera automatisée et l'intervention humaine sera réduite à une validation rapide.

Quatrièmement, afin d'être conforme à la Constitution, le *money control* doit également prévoir une communication *a posteriori*. C'est important pour le contrôle judiciaire *a posteriori*, car si les personnes saisissent la justice, elles doivent pouvoir le faire de manière correcte.

D'autres éléments manquent dans la législation du ministre: le droit à une explication, à des informations significatives sur la logique, le droit à la correction des inexactitudes factuelles et le droit de contester le résultat. Ce sont autant d'éléments qui ne figurent pas dans les sept paragraphes du projet de texte et qui le rendent très vulnérable sur le plan constitutionnel. M. Van Quickenborne se demande, à cet égard, si telle n'est pas, en réalité, la véritable intention du ministre Jambon. Peut-être espère-t-il secrètement être débarrassé du *money control* en cas d'annulation par la Cour constitutionnelle et ainsi être débarrassé de ce caillou que Vooruit a mis dans sa chaussure.

In de tekst is er ook nergens sprake van een zeer strikte bewaartermijn. Er staan wel – in de eerste of de tweede alinea van de tekst – bezwaarlijk strikte termijnen van één jaar, maar die zijn verbonden aan drie cumulatieve voorwaarden, waardoor die bewaring soms tien tot twintig jaar kan blijven aanslepen.

Wat ook niet voorzien is in de tekst, is de problematiek van de login. Er wordt nergens vermeld dat, als men de gegevens heeft gecontroleerd in de vorm van datamining, een belastingplichtige dat kan zien. Evenmin is voorzien reproduceerbaarheid en onafhankelijke audits, inclusief bias- en foutpositieve analyses.

Tenslotte wordt er ook niks gezegd over de versterking van de rol van de GBA via een voorafgaand advies. *Data protection Impact Assessment* (DPIA), goedkeuring voor modellen, doorlopend toezicht en sanctiemogelijkheden. Dat ontbreekt allemaal.

Dus het lijstje van zaken die in die wet zouden moeten staan om grondwettelijk conform te zijn, is behoorlijk lang. Daar wordt niks aan gedaan, wat de tekst bijzonder kwetsbaar maakt voor het Grondwettelijk Hof. Iets waarmee de minister, volgens de spreker, toch rekening mee moet houden.

Dus de grondwettelijke toets die had moeten gebeuren, is niet gebeurd. Ten aanzien van een passief register is er legaliteit nodig. Dat bestaat, via die wet, maar er is meer precisie nodig over de legaliteit. Het doel is wel legitiem, maar is veel te breed. Het is breder dan wat men noemt de ernstige en georganiseerde fraude.

Wat de proportionaliteit betreft, is de noodzakelijkheid twijfelachtig. En ook de evenredigheid is afhankelijk van de waarborgen. De scheiding der machten wordt niet gerespecteerd, er is een gebrek aan *ex ante* onafhankelijke toets en artikel 13 van de Grondwet staat onder druk door onwetendheid over raadplegingen.

De conclusie is dus dat het passieve CAP zoals het nu is, houdbaar is, mits nauwe doelbinding en versterking van de waarborgen, maar structureel wel kwetsbaar.

De spreker verwijst nogmaals naar het arrest van het Grondwettelijk Hof van 2022, waarin het Hof alsnog positief had geoordeeld. Opvallend in dat arrest – dat eigenlijk over de saldi ging – was de vraag of de toevoeging van de saldi wel proportioneel was. In dit opzicht onderstreept het Hof dat daarover misschien discussie kan bestaan, maar dat er zekerheid is over het feit dat

De plus, le texte ne mentionne nulle part une durée de conservation très stricte. Il mentionne bien, dans le premier ou le deuxième paragraphe, des délais d'un an difficilement qualifiables de stricts, mais ceux-ci sont associés à trois conditions cumulatives, ce qui signifie que la conservation pourra parfois atteindre dix ans.

Le texte ne traite pas non plus de la problématique de la connexion. Il n'est mentionné nulle part que le contribuable pourra savoir que ses données ont été contrôlées lors d'un *data mining*. Il ne prévoit pas non plus la reproductibilité, ni des audits indépendants incluant des analyses de biais et de faux positifs.

Enfin, il ne contient aucune disposition sur le renforcement du rôle de l'APD par le biais d'un avis préalable, ni sur une analyse d'impact relative à la protection des données (AIPD), la validation des modèles, le contrôle permanent ou les possibilités de sanction.

La liste des éléments qui devraient figurer dans cette loi pour qu'elle soit conforme à la Constitution est donc assez longue. Rien n'ayant été fait pour qu'elle le soit, ce texte sera particulièrement vulnérable devant la Cour constitutionnelle. L'intervenant estime que le ministre devrait en tenir compte.

En d'autres termes, le contrôle constitutionnel qui aurait dû être réalisé n'a pas eu lieu. Or, la légalité est nécessaire pour un registre passif. Elle a été prévue par la loi à l'examen, mais il conviendra de la préciser. L'objectif est légitime, mais sa définition est beaucoup trop large. Elle va au-delà de ce que l'on appelle la fraude grave et organisée.

En ce qui concerne la proportionnalité, la nécessité est discutable. En outre, la proportionnalité dépend des garanties. La séparation des pouvoirs n'est pas respectée. Le contrôle indépendant *ex ante* fait défaut. Le respect de l'article 13 de la Constitution ne sera pas assuré en raison de l'absence d'informations concernant les consultations.

En conclusion, le PCC passif tel qu'il existe actuellement sera viable, moyennant une limitation stricte de la finalité et un renforcement des garanties, mais il sera structurellement vulnérable.

L'intervenant renvoie de nouveau à l'arrêt rendu par la Cour constitutionnelle en 2022, dans lequel celle-ci avait encore émis un avis favorable. La question principale de cet arrêt, qui portait en réalité sur les soldes, était de savoir si l'ajout de ces soldes était effectivement proportionné. À cet égard, la Cour souligne que ce point pourrait prêter à discussion, mais qu'il ne fait aucun

controle toegelaten is als er voorafgaande aanwijzingen zijn van belastingontduiking.

Dat is eigenlijk een soort buffer, die ervoor zorgt dat die gegevens toch proportioneel worden gehouden. Maar met de komst van *money control* is die buffer natuurlijk helemaal uitgeschakeld en zal het Grondwettelijk Hof uiteraard veel kritischer zijn.

In het geval van profilering en *money control* moet er een veel striktere finaliteit zijn. Er moet een zwaardere noodzakelijkheidstoets komen. Want zonder echte menselijke toets, zonder *ex ante* autorisatie en zonder kennisgeving achteraf, is de evenredigheid niet haalbaar. Er is nood aan onafhankelijk toezicht. En er is ook nood aan recht op uitleg, inzage in logica en effectief beroep. Dus zonder diepgaande hertekening is het, wat profilering en *money control* betreft, onverenigbaar met de Grondwet. Er moeten duidelijke en transparante waarborgen toegevoegd worden.

Conclusie: constitutioneel is het CAP geen non-starter. Het steunt op een wet en dient legitieme doelen. Maar door de manier waarop het vandaag ingericht is, met permanente registratie, relatief ruime toegang en zwakke individuele transparantie, staan de waarborgen van artikel 22 van de Grondwet en de grondwettelijke beginselen van legaliteit, proportionaliteit en de scheiding der machten onder druk.

Als passief register is het CAP volgens de spreker houdbaar op voorwaarde dat men de essentiële elementen nauwer vastlegt en de individuele rechtsbescherming reëel maakt. Dus dat betekent een kennisgeving, raadpleging-log en effectief beroep.

Maar als het gaat om profilering en dus *money control* is het in de huidige constellatie niet verenigbaar met de Grondwet. De aard van de inmenging wordt zwaarder, er is nood aan een *ex ante* onafhankelijke toestemming, aan menselijke eindbeslissingen en betekenisvolle uitleg, *ex post* kennisgeving en ook aan daadwerkelijke remedies. Zonder die harde waarborgen wordt de burger een doelwit van data gedreven controle, in strijd met de Grondwet die net de macht begrenst en rechten effectief wil maken.

Tenslotte wijst de heer Van Quickenborne er nog op dat de Grondwet geen rem zet op efficiëntie, maar dat het een richtsnoer is. Het is de ziel van onze rechtsstaat. Het is niet dat de overheid alles kan wat nuttig lijkt, maar dat zij enkel zoveel mag als noodzakelijk is. Zoals aangestipt door collega Mathieu Michel: het is niet

doute que le contrôle est autorisé s'il existe des indices préalables de fraude fiscale.

Il s'agit en fait d'une sorte de "tampon" qui garantit que ces données restent tout de même proportionnées. Dans le cadre du *money control*, ce tampon a toutefois totalement disparu et la Cour constitutionnelle se montrera beaucoup plus critique.

Dans le cas du profilage et du *money control*, la finalité doit être beaucoup plus stricte. Un test de nécessité plus rigoureux devra être mis en place car sans véritable contrôle humain, sans autorisation *ex ante* et sans notification *ex post*, la proportionnalité est un objectif irréaliste. Un contrôle indépendant est nécessaire, au même titre qu'un droit à des explications, un accès à la logique sous-jacente et un recours effectif. Sans remaniement approfondi, le profilage et le *money control* sont incompatibles avec la Constitution. Des garanties explicites et transparentes doivent être intégrées.

En conclusion, d'un point de vue constitutionnel, le PCC n'est pas inenvisageable. Il s'appuie sur une loi et poursuit des objectifs légitimes. Toutefois, en raison de sa conception actuelle, qui prévoit un enregistrement permanent, un accès relativement large et une transparence individuelle médiocre, les garanties offertes par l'article 22 de la Constitution ainsi que les principes constitutionnels de légalité, de proportionnalité et de séparation des pouvoirs sont fragilisés.

L'intervenant considère que le PCC sera viable en tant que registre passif, à condition que ses éléments essentiels soient définis de manière plus précise et que la protection juridique individuelle devienne une réalité. Cela implique dès lors une notification, un journal des consultations et un recours effectif.

Or, lorsqu'il s'agit de profilage et donc de *money control*, dans sa configuration actuelle, le PCC n'est pas compatible avec la Constitution. Compte tenu du degré élevé d'ingérence, il est nécessaire de prévoir une autorisation indépendante *ex ante*, des décisions finales humaines, une explication significative, une notification *ex post* ainsi que de véritables voies de recours. Sans ces garanties robustes, le citoyen deviendra la cible du contrôle guidé par des données, ce qui est contraire à la Constitution, dont la finalité est précisément de délimiter le pouvoir et de rendre les droits effectifs.

Enfin, M. Van Quickenborne répète que la Constitution ne représente pas un frein à l'efficacité, mais qu'elle constitue un guide. Elle est l'âme de notre État de droit. L'autorité publique ne peut pas faire tout ce qui lui paraît utile, elle ne peut agir que dans les limites de ce qui est nécessaire. Comme l'a souligné Mathieu Michel, ce

omdat technologisch zoveel mogelijk is dat men alles moet kunnen. Het moet altijd proportioneel zijn. Zeker als het gaat over de overheid.

De heer Van Quickenborne vervolgt met een analyse van de Europese regelgeving die een kader schept waaraan de voorliggende maatregelen moeten worden getoetst.

Drie elementen uit de supranationale wetgeving zijn van toepassing op het CAP en bij uitbreiding op amendement nr. 15 (DOC 56 0963/005): de Algemene Verordening Gegevensbescherming (AVG), het Europees Verdrag voor de Rechten van de Mens (EVRM) en het Europees Handvest van de Grondrechten.

I. — HET CAP EN DE ALGEMENE VERORDENING GEGEVENS-BESCHERMING (AVG)

De AVG trad in werking op 25 mei 2018 en vormt het centrale normatieve kader voor elke verwerking van persoonsgegevens binnen de EU. Een verordening heeft rechtstreekse werking: elke nationale regeling die persoonsgegevens verwerkt, ook wanneer zij voortvloeit uit een specifieke wettelijke regeling of verplichting, moet in overeenstemming zijn met de bepalingen en beginselen van de AVG.

Het CAP wordt beheerd door de NBB en werd opgericht door de wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van rekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest (hierna: “CAP-wet”). Het centraliseert de identificatiegegevens van alle bankrekeningen en de meeste financiële contracten van natuurlijke en rechtspersonen. De databank wordt geraadpleegd door onder meer de FOD Financiën, de Cel voor Financiële Informatieverwerking (CFI) en het openbaar ministerie. Door zijn aard en omvang vormt het CAP een grootschalige verwerking van persoonsgegevens van gevoelige aard. Daarom valt het systeem onmiskenbaar onder het materiële en territoriale toepassingsgebied van de AVG (artikelen 2 en 3).

De centrale vraag luidt daarom of het CAP in overeenstemming is met de vereisten van de AVG, en of dat bij uitbreiding ook geldt voor *money control*, dat formeel en materieel voortbouwt op het CAP.

n'est pas parce que la technologie offre des possibilités illimitées qu'il ne doit plus exister de limites. L'action doit toujours être proportionnée, à plus forte raison lorsqu'il s'agit de l'autorité publique.

M. Van Quickenborne poursuit en livrant une analyse de la réglementation européenne, qui crée un cadre à la lumière duquel il convient d'évaluer les mesures à l'examen.

Trois textes de la législation supranationale s'appliquent au PCC et, par extension, à l'amendement n° 15 (DOC 56 0963/005): le règlement général sur la protection des données (RGPD), la Convention européenne des droits de l'homme (CEDH) et la Charte européenne des droits fondamentaux.

I. — LE PCC ET LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

Le RGPD est entré en vigueur le 25 mai 2018 et constitue le cadre normatif de base pour tout traitement de données à caractère personnel au sein de l'Union européenne. Les règlements ayant un effet direct, toute réglementation nationale impliquant le traitement de données à caractère personnel, même si elle découle d'une disposition ou d'une obligation légale spécifique, doit respecter les dispositions et les principes du RGPD.

Le PCC est géré par la BNB et a été créé par la loi du 8 juillet 2018 portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt (ci-après: “loi relative au PCC”). Il centralise les données d'identification de tous les comptes bancaires et de la plupart des contrats financiers des personnes physiques et morales. La base de données est notamment consultée par le SPF Finances, la Cellule de traitement des informations financières (CTIF) et le ministère public. Compte tenu de sa nature et de son ampleur, le PCC constitue un traitement à grande échelle de données à caractère personnel sensibles, raison pour laquelle ce système relève indéniablement du champ d'application matériel et territorial du RGPD (articles 2 et 3).

La question centrale à se poser est dès lors celle de savoir si le PCC est conforme aux exigences du RGPD et, par extension, s'il en va de même pour le *money control*, qui s'appuie formellement et matériellement sur le PCC.

— *Toepassingsgebied van de AVG en de kwalificatie van het CAP*

Artikel 4 van de AVG definieert persoonsgegevens als “alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon”. Verwerking wordt omschreven als “een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés [...]”.

De minister heeft verklaard dat de SAS-software voor datamining geen automatische verwerking beoogt en dat het probleem bijgevolg niet aan de orde is. De definitie van “verwerking” in de AVG betreft echter ook niet-geautomatiseerde processen.

Het CAP verzamelt wel degelijk persoonsgegevens: identificatie van de houder, naam, geboortedatum, rijksregisternummer en adres. Ook gegevens over financiële instellingen, rekeningnummers en data van opening en afsluiting, contracten, leningen, verzekeringen, beleggingsrekeningen en saldi zijn persoonsgegevens. De opname, opslag, koppeling en raadpleging door de NBB en andere autoriteiten vormen verwerking in de zin van artikel 4 van de AVG.

Volgens hetzelfde artikel 4 is de verwerkingsverantwoordelijke degene die het doel en de middelen voor de verwerking vaststelt. De CAP-wet wijst de NBB aan als beheerder van het CAP, maar de fiscale en gerechtelijke autoriteiten bepalen de concrete doeleinden van de raadpleging.

De situatie is complex en gedeeld:

- De NBB is verwerkingsverantwoordelijke voor het beheer en de beveiliging van de databank.
- De FOD Financiën, de CFI, het parket en andere informatiegerechtigden treden op als afzonderlijke verwerkingsverantwoordelijken bij raadpleging.
- Banken zijn verplicht informatie aan te leveren aan het CAP en zijn in die zin een derde groep van verwerkingsverantwoordelijken.

Deze complexe constructie impliceert gedeelde verantwoordelijkheid (zoals voorzien in artikel 26 AVG) en vereist een duidelijke afbakening van de rollen.

— *Champ d'application du RGPD et qualification du PCC*

L'article 4 du RGPD définit les données à caractère personnel comme “toute information se rapportant à une personne physique identifiée ou identifiable [...]”. Le traitement est défini dans ce même article comme “toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel [...]”.

Le ministre a indiqué que le logiciel SAS utilisé pour le *data mining* ne visait pas un traitement automatique et qu'il ne posait dès lors pas de problème. Or, la définition de “traitement” inscrite dans le RGPD concerne également les processus non automatisés.

Le PCC collecte bel et bien des données à caractère personnel: identification du titulaire, nom, date de naissance, numéro de registre national et adresse. Les données relatives aux établissements financiers, aux numéros de compte, aux dates d'ouverture et de fermeture, aux contrats, aux prêts, aux assurances, aux comptes de placement et aux soldes sont également des données à caractère personnel. L'encodage, le stockage, le couplage et la consultation de données par la BNB et d'autres autorités constituent un traitement au sens de l'article 4 du RGPD.

Conformément à ce même article 4, le responsable du traitement est celui qui détermine les finalités et les moyens du traitement. La loi relative au PCC désigne la BNB comme gestionnaire du PCC, mais ce sont les autorités fiscales et judiciaires qui déterminent les finalités concrètes de la consultation.

La situation est complexe et les responsabilités partagées:

- La BNB est responsable du traitement pour la gestion et la sécurisation de la base de données.
- Le SPF Finances, la CTIF, le parquet et les autres personnes habilitées à recevoir l'information agissent en tant que responsables du traitement distincts lors de la consultation.
- Les banques sont obligées de fournir certaines informations au PCC et constituent, à ce titre, un troisième groupe de responsables du traitement.

Cette construction complexe implique une responsabilité partagée (conformément à l'article 26 du RGPD) et requiert une délimitation claire des rôles.

— *Juridische grondslag van het CAP onder artikel 6 AVG*

Elke verwerking moet gebaseerd zijn op één van de voorwaarden van artikel 6, lid 1 AVG. Voor het CAP beroept de Belgische wetgever zich op:

- Artikel 6, lid 1, punt c): “de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust”;

- Artikel 6, lid 1, punt e): “de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen”.

Artikel 6 vereist bovendien dat de nationale wetgeving de specifieke doeleinden van de verwerking bepaalt en passende waarborgen biedt. Dit is een cruciaal element: het EU-recht laat nationale regelingen toe, maar enkel indien zij voldoende precies, voorspelbaar en proportioneel zijn.

Een toetsing aan de Belgische wetgeving leert dat de huidige CAP-wet de volgende vier doeleinden vermeldt: bestrijding van fiscale fraude, toepassing van de antiwitwaswetgeving, ondersteuning van gerechtelijke onderzoeken en uitvoering van opdrachten van algemeen belang door de NBB. De wettelijke grondslag lijkt op die manier vervuld, maar blijft zeer ruim geformuleerd. Er is geen hiërarchie of concrete afbakening van de doeleinden, waardoor secundair gebruik mogelijk blijft (bijvoorbeeld voor statistiek of beleidsanalyse).

De GBA en het Hof van Justitie van de EU hebben herhaaldelijk benadrukt dat vage of meervoudige doelstellingen indruisen tegen de vereisten van artikel 6, lid 3, gelezen in samenhang met artikel 5, lid 1, punt b) AVG. De spreker verwijst naar het arrest *Digital Rights Ireland Ltd tegen minister for Communications, Marine and Natural Resources e.a.* (C-293/12).

— *Analyse van de AVG-beginselen*

De heer Van Quickenborne stipt als eerste beginsel de doelbinding aan: “Persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt” (artikel 5, lid 1, punt b)).

In het kader van de vier voormelde hoofddoeleinden opgenomen in de CAP-wet kan de dataset worden

— *Fondement juridique du PCC en application de l'article 6 du RGPD*

Tout traitement doit reposer sur l'une des conditions prévues à l'article 6, paragraphe 1, du RGPD. Dans le cadre du PCC, le législateur belge invoque les fondements suivants:

- article 6, paragraphe 1, point c): “le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis”;

- article 6, paragraphe 1, point e): “le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement”.

L'article 6 exige en outre que la législation nationale fixe les finalités spécifiques du traitement et qu'elle prévoie des garanties appropriées. Il s'agit d'un élément crucial: le droit de l'Union européenne autorise les réglementations nationales, mais uniquement si elles sont suffisamment précises, prévisibles et proportionnées.

Il ressort de l'examen de la législation belge que la loi actuelle relative au PCC mentionne les quatre finalités suivantes: lutte contre la fraude fiscale, application de la législation anti-blanchiment, soutien dans le cadre des instructions judiciaires et exécution de missions d'intérêt public par la BNB. Le fondement légal semble ainsi fixé, mais il reste formulé de manière très large. Il ne prévoit pas de hiérarchie ni de délimitation concrète des finalités, ce qui laisse la porte ouverte à une utilisation secondaire (par exemple à des fins statistiques ou d'analyse politique).

L'APD et la Cour de justice de l'UE ont souligné à plusieurs reprises que des objectifs vagues ou multiples sont contraires aux exigences de l'article 6, paragraphe 3, lu en combinaison avec l'article 5, paragraphe 1, point b), du RGPD. L'intervenant renvoie à ce propos à l'arrêt *Digital Rights Ireland Ltd contre minister for Communications, Marine and Natural Resources e.a.* (C-293/12).

— *Analyse des principes du RGPD*

M. Van Quickenborne mentionne en premier lieu le principe de limitation des finalités: “Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités” (article 5, paragraphe 1, point b)).

Conformément aux quatre finalités principales précitées, qui figurent dans la loi relative au PCC, le registre

geraadpleegd door de fiscus, de politie en in sommige gevallen de NBB zelf voor statistische doeleinden. Er is geen waarborg dat gegevens niet voor andere doeleinden worden gebruikt zodra ze zijn geraadpleegd, hoewel de wetgever later heeft toegevoegd dat derden deze gegevens niet mogen verkrijgen. Op die manier voldoet het CAP formeel aan de AVG.

Ten tweede geldt het beginsel van dataminimalisatie (artikel 5, lid 1, punt c)): persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is. Het Hof van Justitie stelde in zijn arrest van 6 oktober 2020 (*La Quadrature du Net e.a. tegen premier ministre e.a.*, C-511/18) dat algemene en ongedifferentieerde bewaring van gegevens voor alle personen, zonder onderscheid, in strijd is met de noodzakelijkheidstoets van het Unierecht. Het arrest had weliswaar betrekking op telecomgegevens, maar de redenering is volgens de spreker tevens van toepassing op financiële identificatiegegevens.

De vraag is of de Belgische praktijk op het vlak van de omvang proportioneel is, aangezien de overheid voorafgaandelijk data verzamelt over de hele bevolking, zonder concrete aanleiding.

Ook het derde beginsel, de bewaarbeperking (artikel 5, lid 1, punt e)), is relevant: persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk. De CAP-wet en het voorliggende amendement nr. 15 leggen een bewaartermijn vast, maar de vraag is of die termijn niet te ruim is. Er werd ook nergens een verplichting tot periodieke vernietiging of anonimisering voorzien.

Volgens de rechtspraak van het Hof van Justitie (*Digital Rights Ireland*, C-293/12) moeten bewaartermijnen objectieve criteria bevatten, vastgelegd in de wet zelf. Voldoen het CAP en bij uitbreiding *money control* daar volgens de minister aan?

Verder geldt als vierde principe het transparantiebeginsel (artikelen 12–14 AVG): betrokkenen moeten duidelijk geïnformeerd worden over het doel van de verwerking, de ontvangers van de gegevens en hun rechten (inzage, correctie en bezwaar). Bij het openen van een bankrekening dient de bank de betrokkene in te lichten dat zijn gegevens in het CAP worden opgeslagen. Het is echter onduidelijk of over datamining zoals voorzien in het voorliggende amendement nr. 15 eveneens transparant wordt gecommuniceerd. De tekst bevat geen enkele bepaling dienaangaande, wat betekent dat burgers niet

peut être consulté par le fisc, par la police et, dans certains cas, par la BNB elle-même à des fins statistiques. Rien ne garantit donc que les données ne seront pas utilisées à d'autres fins dès qu'elles auront été consultées, même si le législateur a ajouté ultérieurement que les tiers ne peuvent pas accéder à ces données. De cette manière, le PCC est formellement conforme au RGPD.

M. Van Quickenborne aborde ensuite le principe de minimisation des données (article 5, paragraphe 1, point c)): "Les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire". Dans son arrêt du 6 octobre 2020 (*La Quadrature du Net e.a. contre premier ministre e.a.*, C-511/18), la Cour de justice a estimé que la conservation généralisée et indifférenciée des données pour toutes les personnes, sans distinction, est contraire au critère de nécessité prévu par le droit de l'Union. Même si cet arrêt concernait des données de télécommunications, le raisonnement s'applique également, selon l'intervenant, aux données d'identification financières.

Il convient en outre de se demander si la pratique belge est proportionnée dans son étendue, dès lors que les autorités publiques collectent préalablement des données sur l'ensemble de la population, sans motif concret.

Le troisième principe, à savoir la limitation de la conservation (article 5, paragraphe 1, point e)), est lui aussi pertinent: les données à caractère personnel ne peuvent être conservées plus longtemps que nécessaire. La loi relative au PCC et l'amendement n° 15 à l'examen fixent un délai de conservation, mais la question est de savoir si ce délai n'est pas trop long. Par ailleurs, aucune obligation de destruction périodique ou d'anonymisation n'est prévue.

Selon la jurisprudence de la Cour de justice (*Digital Rights Ireland*, C-293/12), les durées de conservation doivent être fondées sur des critères objectifs fixés dans la loi elle-même. Le ministre estime-t-il que le PCC et, par extension, le contrôle des flux financiers respecteront cette exigence?

Le quatrième principe est celui de la transparence (articles 12 à 14 du RGPD): les personnes concernées doivent être clairement informées de la finalité du traitement, des destinataires des données et de leurs droits (accès, rectification et opposition). Lors de l'ouverture d'un compte bancaire, la banque devra informer la personne concernée que ses données seront enregistrées dans le PCC. Il est difficile de déterminer si celle-ci sera également informée en toute transparence du *data mining* prévu par l'amendement n° 15 à l'examen. Le texte ne contient aucune disposition à cet égard, ce qui signifie

weten dat hun rekeningen en saldi gebruikt worden voor datamining, wie deze gegevens heeft geraadpleegd en of deze raadpleging regelmatig was.

Wellicht zal de minister tegenwerpen dat een publicatie in het *Belgisch Staatsblad* volstaat. Volgens de AVG bestaat echter wel degelijk de verplichting om de betrokkenen expliciet in te lichten. Voldoet *money control* aan deze principes van transparantie, vervat in de artikelen 12 t.e.m. 14 van de AVG?

Tot slot vormen de rechten van betrokkenen (artikelen 15 - 23 AVG) het vijfde beginsel. Het betreft rechten op inzage, rectificatie, beperking, bezwaar en wissen. Artikel 23 laat lidstaten toe deze rechten te beperken voor zover dat noodzakelijk is voor fiscale en strafrechtelijke doeleinden. België heeft zich op dit artikel beroepen: de CAP-wet bepaalt dat de betrokkene geen recht heeft op kennisgeving of inzage wanneer de gegevensverwerking plaatsvindt voor fiscale of gerechtelijke doeleinden.

Dit is juridisch aanvaardbaar op voorwaarde dat de beperking in de wet is voorzien, de wezenlijke inhoud van het recht wordt geëerbiedigd en de beperking noodzakelijk en evenredig is. Aan de eerste voorwaarde is voldaan, maar de tweede en derde zijn minder zeker. Er ontbreken compenserende waarborgen in de bestaande wetgeving, zoals onafhankelijke controle of kennisgeving achteraf. Ook is er geen evaluatie van de proportionaliteit per doeleinde.

Het Hof van Justitie oordeelde in *Tele2 Sverige AB tegen Post- och telestyrelsen* (C-203/15) dat algemene gegevensbewaring zonder individuele beoordeling niet noodzakelijk is in de zin van het EU-recht. Ook op dat vlak lijkt de bestaande regeling de rechten van betrokkenen te schenden.

— *De uitzondering van artikel 23 AVG en de Belgische praktijk*

België heeft artikel 23 AVG ruim toegepast en zelfs geïncorporeerd als permanente uitzondering in het CAP-kader. De spreker stelt zich daar vragen bij: artikel 23 vereist immers een evenwichtige beperking, en geen een structurele uitsluiting zoals België heeft ingevoerd.

que les citoyens ignoreront que leurs comptes et leurs soldes seront utilisés à des fins de *data mining* et qu'ils ignoreront également qui aura consulté leurs données et si cette consultation aura été régulière.

Le ministre objectera sans doute qu'une publication au *Moniteur belge* suffit. Le RGPD prévoit toutefois l'obligation d'informer explicitement les personnes concernées. Le *money control* satisfait-il à ces principes de transparence contenus aux articles 12 à 14 du RGPD?

Enfin, les droits des personnes concernées (articles 15 à 23 du RGPD) constituent le cinquième principe. Il s'agit du droit d'accès, du droit de rectification, du droit à la limitation du traitement, du droit d'opposition et du droit à l'effacement. L'article 23 permet aux États membres de limiter la portée de ces droits pour autant que cette limitation constitue une mesure nécessaire pour répondre à des finalités fiscales et de justice pénale. La Belgique a invoqué cet article: la loi relative au PCC dispose que la personne concernée n'a aucun droit en matière de notification ou de consultation lorsque le traitement de données poursuit une finalité fiscale ou judiciaire.

Cette position est juridiquement acceptable pour autant que la limitation soit prévue dans la loi, que l'essence du droit soit respectée et que la mesure soit nécessaire et proportionnée. S'il est satisfait à la première condition, il est moins certain que la deuxième et la troisième conditions soient également remplies. La législation existante ne prévoit pas de garanties compensatoires, comme un contrôle indépendant ou une notification *a posteriori*. Il n'y a pas non plus d'évaluation de la proportionnalité par objectif.

Dans l'affaire *Tele2 Sverige AB contre Post- och telestyrelsen* et *Secretary of State for the Home Department contre Tom Watson e.a.* (C-203/15), la Cour de justice a estimé qu'une obligation générale de conservation des données sans évaluation individuelle n'était pas nécessaire au sens du droit de l'Union. Sur ce plan également, la réglementation existante semble violer les droits de la personne concernée.

— *L'exception contenue à l'article 23 du RGPD et la pratique belge*

La Belgique a largement appliqué l'article 23 du RGPD au point d'en faire une exception permanente dans le cadre du PCC. L'intervenant s'interroge à cet égard. L'article 23 exige en effet que la limitation soit proportionnée et ne prévoit pas d'exclusion structurelle comme celle qui a été instaurée en Belgique.

Daarnaast ontbreekt een objectieve proportionaliteitsafweging. De CAP-wet motiveert niet waarom permanente opslag en brede toegang noodzakelijk zijn.

Artikel 52 van het Handvest van de Grondrechten bepaalt ten slotte dat beperkingen slechts mogen “voor zover zij noodzakelijk zijn en beantwoorden aan doelstellingen van algemeen belang”. Het CAP doorstaat deze toets niet. De Europese Toezichthouder voor gegevensbescherming (EDPS) beklemtoonde in 2021 dat lidstaten artikel 23 AVG niet mogen gebruiken om structurele ondoorzichtigheid te legitimeren.

— *Data Protection Impact Assessment (DPIA)*

Artikel 35 AVG verplicht verwerkingsverantwoordelijken een DPIA uit te voeren voor verwerkingen die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen.

De kenmerken van het CAP (grootschalige, systematische, gevoelige en langdurige gegevensverwerking) voldoen aan deze criteria. De toenmalige Privacycommissie eiste in haar advies nr. 15/2018 dat een DPIA zou worden uitgevoerd vóór de inwerkingtreding van de CAP-wet. De FOD Financiën verklaarde dat er een DPIA *ex post* werd opgesteld, maar dit werd niet openbaar gemaakt en niet aan de Privacycommissie voorgelegd. Daardoor is het onduidelijk of de risicoanalyse conform artikel 35, lid 7 AVG werd uitgevoerd (systematische beschrijving van de verwerkingen, beoordeling van noodzaak en evenredigheid, en maatregelen om risico's te beperken).

— *Toezicht en accountability*

Artikel 51 AVG verplicht lidstaten een onafhankelijke toezichthouder aan te wijzen. In België vervult de GBA deze taak. Formeel heeft de GBA toezicht op de CAP-wet, maar in de praktijk oefent zij enkel *ex post* controle uit. Zij beschikt niet over structurele toegang tot de logs van het CAP en ontvangt geen periodieke rapportering van de NBB.

De accountability-verplichting van artikel 5, lid 2 AVG (de verwerkingsverantwoordelijke moet kunnen aantonen dat hij de beginselen naleeft) blijft daardoor grotendeels theoretisch.

Par ailleurs, l'appréciation objective de la proportionnalité fait également défaut. La loi relative au PCC ne justifie pas pourquoi il est nécessaire de conserver les données en permanence, ni de les soumettre à un large accès.

Enfin, l'article 52 de la Charte des droits fondamentaux dispose que “des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général”. Le PPC ne répond pas à cette condition. En 2021, le Contrôleur européen de la protection des données (CEPD) a rappelé que les États membres ne pouvaient pas se prévaloir de l'article 23 du RGPD pour justifier une opacité structurelle.

— *Analyse d'impact relative à la protection des données (AIPD)*

L'article 35 du RGPD oblige le responsable du traitement à effectuer une AIPD lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Or, les caractéristiques du PCC (traitement de données à grande échelle, systématique, à caractère sensible et de longue durée) répondent à ces critères. Dans son avis n° 15/2018, la commission de la protection de la vie privée de l'époque a exigé la réalisation d'une AIPD avant que la loi relative au PCC entre en vigueur. Le SPF Finances a déclaré qu'une AIPD a été réalisée *ex post*, mais celle-ci n'a pas été rendue publique et n'a pas été soumise à la commission de la protection de la vie privée. En conséquence, on ne sait pas clairement si l'analyse des risques a été effectuée conformément à l'article 35, alinéa 7, du RGPD (description systématique des opérations de traitement, évaluation de la nécessité et de la proportionnalité de celles-ci et mesures envisagées pour faire face aux risques).

— *Surveillance et responsabilité*

L'article 51 du RGPD oblige les États membres à désigner une autorité de contrôle indépendante. En Belgique, cette tâche est assurée par l'APD. Formellement, l'APD veille au respect de la loi relative au PCC, mais dans la pratique, elle n'exerce qu'un contrôle *a posteriori*. Elle ne dispose pas d'un accès structurel aux logs du PCC et ne reçoit pas de rapports périodiques de la BNB.

L'obligation de responsabilité prévue à l'article 5, paragraphe 2, du RGPD (le responsable du traitement doit pouvoir démontrer qu'il respecte les principes) reste donc en grande partie théorique.

— *Compliance versus proportionaliteit*

De Belgische wetgever heeft bij de invoering van het CAP in 2018 rekening gehouden met advies nr. 15/2018 van de Privacycommissie: er is een wettelijke basis, de NBB is aangeduid als verwerkingsverantwoordelijke, logging en beveiliging zijn voorzien en een beperkt inzage-recht is erkend. Op papier lijkt de regeling conform de artikelen 6 en 24 - 32 AVG.

De vraag is echter of er geen materiële tekortkomingen schuilgaan achter deze formele conformiteit. Inhoudelijk schiet de regeling tekort ten aanzien van de fundamentele beginselen van de AVG:

1. Er ontbreekt een noodzakelijkheidstoets per doel: het CAP werkt preventief en algemeen, niet reactief en individueel.
2. Er is geen effectieve transparantie of rechtsmiddel: burgers weten niet waarom gegevens worden geraadpleegd.
3. Er is gebrek aan onafhankelijke *ex ante* controle: de toegang is administratief, zonder rechterlijke of externe toetsing.
4. Er is ruim gebruik van data: de NBB mag gegevens ook verwerken voor statistische doeleinden.
5. Bewaartermijnen zijn weliswaar wettelijk vastgelegd, maar zeer ruim geformuleerd.

Deze tekortkomingen leiden tot een systeem dat formele AVG-compliance claimt, maar materieel de geest van de AVG ondermijnt.

— *Samenvatting: juridische beoordeling van het CAP onder de AVG*

De verhouding tussen CAP en AVG kan in vier dimensies worden samengevat:

1. Wettelijke grondslag: artikel 6, lid 1, punten c) en e) vereisen een specifieke wet met nauw omschreven doel. De CAP-wet voldoet, maar met te ruime finaliteiten.
2. Doelbinding en minimalisatie: artikel 5, lid 1, punten b) en c) vereisen dat enkel noodzakelijke gegevens worden verwerkt. Het CAP registreert alle burgers, ongeacht het risico, wat disproportioneel lijkt.

— *Conformité vs proportionnalité*

Lors de l'instauration du PCC en 2018, le législateur belge a tenu compte de l'avis 15/2018 de la Commission de la protection de la vie privée: il existe une base légale, la BNB est désignée comme responsable du traitement, un login et des mesures de sécurité sont prévues et un droit d'accès limité est reconnu. Sur le papier, la réglementation semble conforme aux articles 6 et 24 à 32 du RGPD.

La question est toutefois de savoir si cette conformité formelle ne cache pas des lacunes matérielles. Sur le fond, la réglementation ne répond pas aux principes fondamentaux du RGPD:

1. Il n'y a pas d'évaluation de la nécessité par objectif: le PCC procède de manière préventive et générale, et non de manière réactive et individuelle.
2. Il n'y a pas de transparence ni de voie de recours effectives: les citoyens ne savent pas pourquoi les données sont consultées.
3. Il n'y a pas de contrôle indépendant *ex ante*: l'accès est administratif, sans contrôle juridictionnel ou externe.
4. Les données sont largement utilisées: la BNB peut également traiter des données à des fins statistiques.
5. Les délais de conservation sont certes fixés par la loi, mais en des termes très vagues.

Ces lacunes conduisent à un système qui prétend être conforme au RGPD sur le plan formel, mais qui, dans les faits, sape l'esprit de ce règlement.

— *Résumé: évaluation juridique du PCC à la lumière du RGPD*

L'articulation entre le PCC et le RGPD peut être résumée en quatre points:

1. Base légale: l'article 6, paragraphe 1^{er}, points c) et e), impose d'adopter une loi spécifique poursuivant un objectif clairement défini. La loi relative au CAP est conforme à ce critère, mais ses finalités sont trop larges.
2. Limitation de la finalité et minimisation des données: l'article 5, paragraphe 1^{er}, points b) et c), impose que seules les données nécessaires soient traitées. Or, le PCC enregistre tous les citoyens, quel que soit le risque, ce qui semble disproportionné.

3. Transparantie en rechten: artikelen 12–13 behandelen kennisgeving, inzage en bewaring. Het CAP voorziet structurele uitsluiting bij fiscale en gerechtelijke doeleinden, wat problematisch is, gelet op het evenredigheidsbeginsel.

4. Toezicht en DPIA: artikelen 35 en 51 vereisen risicobeoordeling en onafhankelijk toezicht. Het CAP voldoet hier onvoldoende: het DPIA is niet openbaar en het toezicht door de GBA gebeurt *ex post*.

De kern van de spanning ligt in het verschil tussen formele naleving van de AVG en de geest van deze Verordening. Het CAP voldoet formeel aan het kader, maar past het volgens de spreker op cruciale punten te breed toe. Het resultaat is een systeem van *ex ante* dataverzameling dat zich juridisch op de AVG beroept, maar materieel de kernbeginselen van noodzakelijkheid en evenredigheid ondermijnt.

— Conclusie CAP en AVG

Het CAP lijkt formeel verenigbaar met de AVG, maar materieel problematisch. Het systeem schiet tekort op het vlak van noodzakelijkheid, proportionaliteit, transparantie en onafhankelijke controle. Het Hof van Justitie heeft in meerdere arresten benadrukt dat algemene en ongedifferentieerde opslag van persoonsgegevens niet toelaatbaar is, ongeacht het doel dat zij nastreven. Het CAP bevindt zich dus op een spanningsveld (formeel conform, maar inhoudelijk strijdig met de geest van de AVG) en is in die zin een testcase voor de grenzen van de AVG in de context van financiële surveillance.

II. — HET CAP EN HET EUROPEES VERDRAG VOOR DE RECHTEN VAN DE MENS (EVRM)

Het EVRM is een constitutionele minimumstandaard die het grondwettelijke referentiekader voor fundamentele rechten in Europa vormt. België is onderworpen aan de toezichtsbevoegdheid van het Europees Hof voor de Rechten van de Mens (EHRM) in Straatsburg.

Elke Belgische wet, inclusief de CAP-wet en de voorliggende amendementen, moet verenigbaar zijn met de waarborgen van het EVRM. De toetssteen bij uitstek is artikel 8 EVRM, dat het recht op eerbiediging van het privéleven beschermt.

De kernvraag is in welke mate de centrale registratie en raadpleging van financiële gegevens in het CAP en

3. Transparence et droits: les articles 12-13 traitent de la notification, de l'accès et de la conservation. Le PCC prévoit une exception structurelle à des fins fiscales et judiciaires, mais c'est problématique au regard du principe de proportionnalité.

4. Contrôle et AIPD: les articles 35 et 51 imposent une évaluation des risques et un contrôle indépendant. Le PCC ne satisfait pas suffisamment à ces exigences: l'AIPD ne sera pas publique et le contrôle par l'APD sera effectué *a posteriori*.

Le nœud du problème réside dans la différence entre le respect formel du RGPD et l'esprit de ce règlement. L'intervenant estime que le PCC respectera ce règlement sur le plan formel, mais l'appliquera trop largement sur plusieurs points cruciaux pour aboutir à un système de collecte de données *ex ante* qui s'appuiera juridiquement sur le RGPD, mais qui, dans les faits, sapera les principes fondamentaux de nécessité et de proportionnalité.

— Conclusion PCC et RGPD

Le PCC semble être formellement conforme au RGPD, mais il pose des problèmes sur le plan matériel. Ce système est inadéquat en matière de nécessité, de proportionnalité et de transparence, et en ce qui concerne l'indépendance du contrôle. La Cour de justice a souligné, dans plusieurs arrêts, que le stockage généralisé et indifférencié de données à caractère personnel n'est pas admissible, quel que soit l'objectif poursuivi. C'est pourquoi le PCC se situe dans une zone de tension (formellement conforme mais contraire, sur le fond, à l'esprit du RGPD). Il constitue, en ce sens, un cas de test en ce qui concerne les limites de ce règlement dans le contexte de la surveillance financière.

II. — LE PCC ET LA CONVENTION EUROPÉENNE DES DROITS DE L'HOMME (CEDH)

La CEDH est une norme constitutionnelle minimale qui constitue le cadre de référence constitutionnel des droits fondamentaux en Europe. La Belgique est soumise au pouvoir de contrôle de la Cour européenne des droits de l'homme (Cour eur. D.H.) de Strasbourg.

Toute loi belge, y compris la législation sur le PCC et les amendements à l'examen, doit être compatible avec les garanties prévues par la CEDH. C'est, par excellence, l'article 8 de la CEDH, qui protège le droit au respect de la vie privée, qui permet de le vérifier.

La question centrale est de savoir dans quelle mesure l'enregistrement centralisé et la consultation des données

bij uitbreiding *money control* te verzoenen zijn met artikel 8 EVRM zoals geïnterpreteerd door het Europees Hof.

— *Artikel 8 EVRM*

Het voornoemde artikel 8 luidt als volgt:

1. Een ieder heeft recht op respect voor zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.

2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.”

Het EHRM hanteert een brede interpretatie van artikel 8. Het beschermt niet alleen het fysieke privéleven, maar ook het informatieve en relationele aspect van privacy: het recht van een individu om te bepalen wie toegang heeft tot persoonlijke informatie, inclusief financiële gegevens. Deze bepalingen zijn bijgevolg tevens van toepassing op het CAP en op *money control*.

— *Zijsporang: Cash Control versus money control*

De spreker verwijst vervolgens naar een artikel in *Moustique* van 31 oktober 2025 (“*Le fisc veut utiliser l’IA pour surveiller nos comptes bancaires: sommes-nous fliqués par des robots?*”) waarin tevens sprake is van een databank met alle voorschriften van artsen om fraude op te sporen in de strijd tegen het hoge aantal langdurig zieken. Een dergelijk systeem zou “*Doctor Control*” genoemd kunnen worden, naar analogie met de door de heer Van Quickenborne gelanceerde benaming *money control* of het door de heer Lode Vereeck (VB) voorgestelde alternatief *Cash Control*.

De heer Lode Vereeck (VB) benadrukt dat de heer Van Quickenborne er goed aan doet bij zijn originele term *money control* te blijven, zodat de draagwijdte duidelijk wordt voor de bevolking.

De benaming *Cash Control* kan dan gereserveerd worden voor de plannen van de EU om het gebruik van cash te beperken en een digitale munt (*Central Bank Digital Currency*, CBDC) te lanceren, waarvan de

financières dans le PCC et, par extension, le *money control* sont conciliables avec l’article 8 de la CEDH tel qu’il est interprété par la Cour européenne.

— *Article 8 de la CEDH*

L’article 8 précité s’énonce comme suit:

“1. “Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d’une autorité publique dans l’exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu’elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l’ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d’autrui.”

La Cour européenne des droits de l’homme applique une interprétation large de l’article 8, qui protège non seulement la vie privée physique, mais également les aspects informatif et relationnel de la vie privée, c’est-à-dire le droit de l’individu à déterminer qui a accès à ses informations personnelles, y compris à ses données financières. Par conséquent, ces dispositions s’appliquent également au PCC et au *money control*.

— *Parenthèse: Cash Control versus money control*

L’intervenant renvoie ensuite à un article paru dans le magazine *Moustique* du 31 octobre 2025 (“*Le fisc veut utiliser l’IA pour surveiller nos comptes bancaires: sommes-nous fliqués par des robots?*”), qui évoque également une banque de données qui centraliserait toutes les prescriptions médicales en vue de détecter les fraudes dans le cadre de la lutte contre le nombre élevé de maladies de longue durée. Ce système pourrait être dénommé “*Doctor Control*”, par analogie avec l’appellation *money control*, proposée par M. Van Quickenborne, ou avec l’appellation *Cash Control*, imaginée par M. Lode Vereeck (VB).

M. Lode Vereeck (VB) souligne que M. Van Quickenborne fait bien de s’en tenir à son appellation originale *money control* pour que la population comprenne bien de quoi il s’agit.

L’appellation *Cash Control* pourrait alors être réservée aux projets de l’Union européenne visant à limiter l’utilisation de l’argent liquide et à mettre en place une monnaie numérique (*Central Bank Digital Currency*, CBDC), la

programmeerbaarheid en de controleerbaarheid van uitgaven vooralsnog onduidelijk zijn.

De bepalingen van amendement nr. 15 zouden uit het wetsontwerp gehaald moeten worden. De minister lijkt door zijn drukke bezigheden het grotere geheel – de evolutie naar een controlemaatschappij – niet meer te zien. Met het schrappen van *chat control* kon een eerste poging afgeweerd worden. *money control* werd echter op slinkse aan het voorliggende wetsontwerp toegevoegd: de meerderheid probeert het onder de vorm van een amendement door te duwen.

Het is de verdienste van de heer Van Quickenborne om erop aan te dringen deze bepalingen uit het wetsontwerp te lichten en er een afzonderlijk uitvoerig debat over te voeren, in plaats van deze discussie in het kader van een wetsontwerp houdende diverse bepalingen te laten plaatsvinden.

De heer Vincent Van Quickenborne (Open Vld) vervolgt met zijn verwijzing naar het voornoemde artikel in *Moustique*, tot nu toe het enige in Franstalig België dat aandacht besteedt aan de voorliggende wetteksten. De heer Florian Jacques, doctorandus aan de Universiteit de Namur, onderzoekt fiscale profilering en roept in het interview op om instrumenten zoals het CAP en data-mining enkel te gebruiken binnen een duidelijk wettelijk kader, dat vandaag ontbreekt.

In het artikel wordt overigens verwezen naar voorstellen van de VB-fractie – een onrechtstreekse pluim voor de heer Vereeck (VB) – om rechtswaARBorgen voor burgers in te bouwen, die volgens de heer Jacques om politieke redenen niet ten gronde worden besproken.

De onderzoeker stipt verder aan dat veel politici niet volledig begrijpen waarover ze beslissen, omdat er vooral interesse is voor de resultaten, zonder zich rekenschap te geven van de risico's.

Aangaande de plannen voor een digitale euro is de heer Van Quickenborne van mening dat er veel kritische vragen kunnen worden gesteld. De digitale euro is zeer privacy-intrusief; een gedachtewisseling met de minister over dat thema zou dan ook zinvol zijn. De term *Cash Control* kan in die context een interessante aanvulling zijn op andere controlemechanismen die gaandeweg worden uitgerold, bijvoorbeeld voor privégesprekken, financiële data en medische gegevens.

programmabilité et la contrôlabilité des dépenses étant encore relativement incertaines.

Les dispositions de l'amendement n° 15 devraient être retirées du projet de loi. Le ministre semble ne plus voir la situation dans son ensemble – l'évolution vers une société de contrôle – tant ses activités sont nombreuses. La suppression du *chat control* a permis de faire barrage à une première tentative, mais le *money control* a toutefois été sournoisement inséré dans le projet de loi à l'examen, la majorité tentant de le faire passer en recourant au subterfuge de l'amendement.

M. Van Quickenborne a le mérite de demander instamment que ces dispositions soient retirées du projet de loi et fassent l'objet d'un débat approfondi séparé, plutôt que d'être discutées dans le cadre de l'examen d'un projet de loi portant des dispositions diverses.

M. Vincent Van Quickenborne (Open Vld) continue de se référer à l'article précité du magazine *Moustique* qui est, à ce jour, la seule publication en Belgique francophone consacrée aux textes de loi à l'examen. M. Florian Jacques, doctorant à l'université de Namur, fait de la recherche sur le profilage fiscal et appelle, dans l'entretien accordé au magazine *Moustique*, à n'utiliser des instruments tels que le PCC et le *data mining* que dans un cadre légal clair, lequel fait défaut actuellement.

L'article adresse d'ailleurs un compliment indirect à M. Vereeck (VB) en évoquant des propositions du groupe VB visant à inclure des garanties juridiques pour les citoyens. Selon M. Jacques, ces propositions n'ont pas été examinées en profondeur pour des raisons politiques.

Le chercheur relève ensuite que beaucoup de responsables politiques ne comprennent pas totalement de quoi ils débattent, parce qu'ils s'intéressent surtout aux résultats, sans tenir compte des risques.

En ce qui concerne les projets d'euro numérique, M. Van Quickenborne estime que de nombreuses réserves peuvent être émises. L'euro numérique représente une intrusion considérable dans la vie privée, si bien qu'il serait opportun d'organiser un échange de vues avec le ministre sur ce sujet. Dans ce contexte, il serait intéressant d'ajouter la notion de *Cash Control*, autrement dit le contrôle des espèces, parmi les mécanismes de contrôle qui sont progressivement déployés, par exemple à l'égard des conversations privées, des données financières et des données médicales.

— *Toepassing van artikel 8 EVRM op financiële gegevens en databanken*

Het EHRM heeft in verschillende arresten erkend dat financiële gegevens onder het begrip “priveleven” vallen. Zo bevestigde het Hof in het arrest *M.S. tegen Zweden* (1997) dat de opslag en verwerking van persoonlijke gegevens, met name van financiële of medische aard, een inmenging betekenen in het privéleven van de betrokkenen.

Het CAP en bij uitbreiding *money control* vormen een inmenging in de zin van artikel 8, zelfs indien de gegevens niet openbaar zijn en geen bedragen bevatten. Inmiddels zijn ook saldi aan het CAP toegevoegd, wat de inmenging nog duidelijker maakt.

— *Voorwaarden in artikel 8, lid 2 EVRM*

De vraag is of deze inmenging gerechtvaardigd kan worden. Artikel 8, lid 2 voorziet die mogelijkheid, zij het onder drie cumulatieve voorwaarden.

1. De inmenging moet bij wet voorzien zijn

Deze voorwaarde omvat drie subvereisten: de toegankelijkheid van de norm, de voorzienbaarheid van de gevolgen en de kwaliteit van de wet. De norm moet voldoende precies zijn en misbruik van bevoegdheid voorkomen.

De CAP-wet van 8 juli 2018 en het voorliggende amendement nr. 15 voldoen formeel aan de eis van toegankelijkheid: ze zijn openbaar en kwamen of komen democratisch tot stand.

De voorzienbaarheid roept echter vragen op. Burgers moeten redelijkerwijs kunnen voorzien onder welke omstandigheden en voorwaarden de overheid toegang krijgt tot hun gegevens. Recente voorbeelden, zoals het dossier van de meerwaardebelasting, tonen aan dat dit principe niet altijd wordt gerespecteerd. De vraag is of de CAP-wet en het voorliggende amendement nr. 15 aan het beginsel beantwoorden.

De huidige CAP-wet bevat immers een ruime categorie van toegangsrechten voor verschillende informatiege-rechtigden (de fiscus, het CFI, het parket). Er is geen voorafgaande rechterlijke toestemming vereist, noch in de wet van 2018, noch in de voorliggende amendementen. Bovendien zal de burger in het systeem van *money control* niet geïnformeerd worden wanneer zijn gegevens worden geraadpleegd.

— *Application de l'article 8 de la CEDH aux données et banques de données financières*

Dans plusieurs arrêts, la Cour européenne des droits de l'homme a reconnu que les données financières relevaient de la vie privée. Elle a ainsi confirmé dans l'arrêt *M.S. c. Suède* (1997) que le stockage et le traitement de données à caractère personnel, de nature financière ou médicale en l'occurrence, constituent une ingérence dans le droit au respect de la vie privée des intéressés.

Le PCC et, par extension, le *money control* constituent une ingérence au sens de l'article 8, même si les données ne sont pas publiques et ne contiennent pas de montants. Entre-temps, les soldes bancaires ont été ajoutés au PCC, ce qui rend l'ingérence encore plus manifeste.

— *Conditions énoncées dans l'article 8, alinéa 2, de la CEDH*

Il convient de se demander si cette ingérence est justifiable. L'article 8, alinéa 2, de la Convention prévoit la possibilité qu'elle le soit, pour autant que trois conditions cumulatives soient remplies.

1. L'ingérence doit être prévue par la loi.

Cette exigence comprend trois sous-conditions: l'accessibilité de la norme, la prévisibilité des conséquences et la qualité de la loi. La norme doit être suffisamment précise et empêcher tout abus de pouvoir.

La loi du 8 juillet 2018 relative au PCC et l'amendement n° 15 à l'examen répondent formellement à l'exigence d'accessibilité: ce sont des normes publiques et elles sont ou ont été élaborées démocratiquement.

En revanche, le critère de la prévisibilité pose question. Les citoyens doivent pouvoir raisonnablement prévoir dans quelles circonstances et conditions les autorités ont accès à leurs données. Des exemples récents, par exemple dans le dossier de la taxe sur les plus-values, montrent que ce principe n'est pas toujours respecté. La question est de savoir si la loi relative au PCC et l'amendement n° 15 à l'examen observent ce principe.

En effet, la loi actuelle relative au PCC prévoit une vaste gamme de droits d'accès pour les différentes personnes habilitées à recevoir l'information (l'administration fiscale, la CTIF, le parquet). Aucune autorisation judiciaire préalable n'est requise, ni dans la loi de 2018, ni dans les amendements à l'examen. En outre, dans le système du *money control*, le citoyen ne sera pas prévenu lorsque ses données sont consultées.

Het EHRM heeft in de zaak *Amann tegen Zwitserland* in 2000 nochtans geoordeeld dat de wetten inzake gegevensverwerking nauwkeurige regels moeten bevatten over de aard van de gegevens, de omstandigheden waaronder ze mogen worden opgeslagen, de procedure voor de raadpleging en de duur van bewaring. Beantwoorden het CAP en de toekomstige regelingen aan deze *quality of law*-standaard?

2. Er moet een legitiem doel bestaan

In artikel 8, lid 2 EVRM wordt een legitiem doel nader omschreven als nationale veiligheid, openbare veiligheid, economisch welzijn en het voorkomen van misdrijven.

Het CAP en *money control* worden door de wetgever verantwoord vanuit het economisch welzijn van het land (belastinginning) en het voorkomen van strafbare feiten zoals fraude en witwassen. Het EHRM aanvaardt deze doeleinden inderdaad als legitiem.

3. Noodzakelijkheid en proportionaliteit

De inmenging moet ten derde proportioneel zijn, beantwoorden aan een dringende maatschappelijke behoefte, evenredig zijn met het doel en voorzien zijn van adequate waarborgen tegen willekeur. Dat wordt onder meer bepaald in de zaak *Klass e.a. tegen Duitsland* (1978). In deze bepaling zit het zwaartepunt van de toepassing van artikel 8 EVRM vervat.

— Relevante EHRM-rechtspraak

De heer Van Quickenborne bespreekt vervolgens enkele belangrijke uitspraken van het EHRM inzake gegevensverwerking.

In *Amann tegen Zwitserland* (2000) werd geoordeeld dat de loutere registratie van gegevens over een burger door een overheidsdienst reeds een inmenging vormt. De wet moet duidelijk omschrijven welke categorieën van gegevens mogen worden bewaard, wie toegang heeft, hoelang en voor welke doeleinden. Beantwoorden de huidige en de toekomstige regels aan deze *quality of law*-vereisten?

In de zaak *Rotaru tegen Roemenië* oordeelde het EHRM in 2000 dat het bijhouden van een register met persoonlijke gegevens over een individu onder artikel 8 EVRM valt. Het ontbreken van duidelijke regels over bewaring, correctie en vernietiging werd gezien als een schending van het Verdrag. De vraag is hoe het zit met het CAP en bij uitbreiding *money control*. Is er een

Or, la CEDH a estimé en 2000, dans l'affaire *Amann c. Suisse*, que les lois applicables au traitement de données doivent contenir des dispositions précises concernant la nature des données, les circonstances dans lesquelles elles peuvent être enregistrées, la procédure relative à leur consultation et la durée de conservation. Le PCC et les futurs régimes sont-ils conformes à cette norme de qualité de la législation?

2. Il doit y avoir un objectif légitime

En vertu de l'article 8, alinéa 2, de la CEDH, la sécurité nationale, la sûreté publique, le bien-être économique et la prévention des infractions pénales constituent un objectif légitime.

Le législateur justifie le PCC et *money control* par le bien-être économique du pays (perception des impôts) et la prévention d'infractions pénales telles que la fraude et le blanchiment d'argent. La CEDH reconnaît effectivement la légitimité de ces objectifs.

3. Nécessité et proportionnalité

Troisièmement, l'ingérence doit être proportionnelle, correspondre à un besoin social impérieux, être proportionnée au but poursuivi et être assortie de garanties adéquates contre l'arbitraire. C'est ce qui a notamment été établi dans l'affaire *Klass et autres c. Allemagne* (1978), et c'est là que réside l'essentiel de l'application de l'article 8 de la CEDH.

— Jurisprudence pertinente de la Cour européenne des droits de l'homme

M. Van Quickenborne aborde ensuite plusieurs arrêts importants rendus par la Cour européenne des droits de l'homme en matière de traitement des données.

Dans l'affaire *Amann c. Suisse* (2000), il a été jugé que le simple enregistrement de données relatives à un citoyen par un service public constitue déjà une ingérence. La loi doit définir clairement les catégories de données qui peuvent être conservées, qui y a accès, pendant combien de temps et à quelles fins. Les règles actuelles et futures répondent-elles à ces exigences de qualité du droit?

Dans l'affaire *Rotaru contre Roumanie*, la Cour européenne des droits de l'homme a estimé en 2000 que la tenue d'un registre contenant des données à caractère personnel relatives à un individu relève de l'article 8 de la CEDH. L'absence de règles claires en matière de conservation, de rectification et de destruction a été considérée comme une violation de la Convention. La

precieze bewaartermijn? Is er een mogelijkheid tot correctie? Is er voorzien in de vernietiging van gegevens?

In het arrest *S. en Marper tegen het Verenigd Koninkrijk* (2008), over het bewaren van DNA en vingerafdrukgegevens van niet-veroordeelden, werd geoordeeld dat algemene en ongedifferentieerde bewaring van gegevens disproportioneel is, zelfs met een legitiem doel. De spreker vraagt zich af waar deze evolutie naar tal van controlemechanismen uiteindelijk zal stoppen, en is verheugd dat het EHRM op zijn minst een rem zet op dergelijke verregaande maatregelen. Is een *a priori* dataverzameling, niet gebaseerd op individuele verdenking, zoals met *money control* gebeurt, wel conform het EVRM?

In de zaak *Zakharov tegen Rusland* (2015) bevestigde het EHRM dat zelfs het loutere bestaan van een wettelijk systeem dat massale toegang tot communicatiegegevens mogelijk maakt een schending van het EVRM kan vormen, ongeacht individueel misbruik. Belangrijker nog, het EHRM eist een onafhankelijke *ex-ante* controle door een rechter of een gelijkwaardige instantie. De conclusie van deze zaak is dat er een onafhankelijk toezicht moet zijn. Dit lijkt niet het geval bij *money control*.

Het lid vervolgt zijn opsomming met de zaak *Big Brother Watch e.a. tegen het Verenigd Koninkrijk* (2021). Het EHRM oordeelde in deze procedure dat *mass surveillance* slechts toelaatbaar is mits *end-to-end*-waarborgen, meer bepaald duidelijke selectiecriteria, voorafgaande goedkeuring, toezicht tijdens de verwerking, kennisgeving achteraf en doeltreffende beroepsmogelijkheden. Het voorliggende amendement nr. 15 voldoet hoegenaamd niet aan deze voorwaarden.

— Beoordeling aan de hand van EHRM-criteria

Voorstanders van *money control* kunnen er maar beter voor zorgen dat de wetgeving robuust genoeg is en de toets van het Grondwettelijk Hof en het EHRM doorstaat. De tekst getuigt echter van amateurisme en dreigt uiteindelijk vernietigd te worden.

Het mechanisme scoort ruimschoots onvoldoende op de criteria van het EVRM inzake legaliteit ("*quality of law*"), de vereiste van duidelijk voorzienbare en toegankelijke

question est de savoir ce qu'il en est du PCC et, par extension, de *money control*. Y-a-t-il un délai de conservation précis? Est-il possible de corriger les données? La destruction des données est-elle prévue?

Dans l'arrêt *S. et Marper c. Royaume-Uni* (2008), concernant la conservation des données ADN et des empreintes digitales de personnes non condamnées, il a été jugé que la conservation générale et indifférenciée de données est disproportionnée, même si elle poursuit un objectif légitime. L'intervenant se demande où s'arrêtera cette évolution tendant vers une multitude de mécanismes de contrôle et se réjouit que la Cour européenne des droits de l'homme mette au moins un frein à ce type de mesures radicales. Une collecte de données *a priori*, non fondée sur des soupçons individuels, comme c'est le cas avec *money control*, est-elle bien conforme à la CEDH?

Dans l'affaire *Zakharov c. Russie* (2015), la Cour européenne des droits de l'homme a confirmé que la simple existence d'un système légal permettant l'accès massif à des données de communication peut constituer une violation de la CEDH, indépendamment de tout abus individuel. Plus important encore, la Cour exige un contrôle indépendant *ex ante* par un juge ou une autorité équivalente. La conclusion de cette affaire est qu'un contrôle indépendant doit être exercé. Cela ne semble pas être le cas avec *money control*.

Le membre poursuit son énumération avec l'affaire *Big Brother Watch et autres contre Royaume-Uni* (2021). Dans cette affaire, la Cour européenne des droits de l'homme a estimé que la surveillance de masse n'était admissible qu'à condition que des "garanties de bout en bout" soient mises en place, à savoir des critères de sélection clairs, une autorisation préalable, un contrôle pendant le traitement, une notification *a posteriori* et des voies de recours efficaces. L'amendement n° 15 à l'examen ne répond absolument pas à ces conditions.

— Évaluation sur la base des critères de la Cour européenne des droits de l'homme

Les partisans de *money control* ont tout intérêt à veiller à ce que la législation soit suffisamment solide et résiste à l'épreuve de la Cour constitutionnelle et de la Cour européenne des droits de l'homme. Le texte témoigne toutefois d'un certain amateurisme et risque d'être annulé *in fine*.

Le mécanisme est largement insuffisant au regard des critères de la Cour européenne des droits de l'homme en matière de légalité ("*quality of law*"), qui exigent des

regels. De doelstellingen zijn te ruim en de toegang is niet limitatief geregeld.

Aan de voorwaarde van een legitiem doel in de zin van artikel 8, lid 2 EVRM kan dan wel voldaan zijn (economisch welzijn en het voorkomen van misdrijven), maar dat betekent nog niet dat de proportionaliteit in orde is. Het doel heiligt niet altijd de middelen.

Wat de kwestie van de noodzakelijkheid betreft is de tekst volstrekt disproportioneel. Alleen onontbeerlijke gegevens mogen worden geregistreerd, en niet massaal of permanent.

Daarnaast moeten er ook waarborgen zijn tegen misbruik en is er nood aan onafhankelijke controle, kennisgeving en mogelijkheid tot beroep. Bij raadpleging van het CAP is enkel logging bij wet geregeld, wat overigens niet is voorzien bij *money control*. Er is geen sprake van onafhankelijke toetsing.

De conclusie op basis van artikel 8 EVRM is dat het Hof vernietigend zal zijn over de voorliggende tekst, behalve op het vlak van het legitieme doel.

— Andere relevante EVRM-bepalingen

Het EVRM bevat voorts het artikel 6, waarin het recht op eerlijk proces is vervat. Wanneer gegevens uit het CAP worden gebruikt in fiscale of strafrechtelijke procedures, rijst de vraag of de betrokkene een eerlijk proces heeft gehad indien hij niet op de hoogte was van de gegevensverzameling die tegen hem wordt gebruikt.

In de zaak *Jalloh tegen Duitsland* (2006) oordeelde het EHRM dat bewijsmateriaal dat verkregen is in strijd met artikel 8 – het recht op eerbiediging van het privéleven – ook gevolgen kan hebben voor artikel 6 – het recht op een eerlijk proces –, zeker wanneer de betrokkene geen mogelijkheid had om het bewijs te betwisten.

Het feit dat het bewijs moeilijk te betwisten valt omdat het algoritme voor datamining in het CAP dusdanig vaag is, vormt reeds een fundamenteel probleem. Artikel 6 van het EVRM komt bijgevolg mogelijk in het gedrang door het systeem van *money control*.

Daarnaast staat in artikel 13 van het EVRM het recht op een doeltreffend rechtsmiddel. Staten zijn verplicht om dit te voorzien in het geval van schending van EVRM-rechten.

règles clairement prévisibles et accessibles. Les objectifs sont trop vastes et l'accès n'est pas réglementé de manière restrictive.

Même si la condition d'un objectif légitime au sens de l'article 8, paragraphe 2, de la CEDH est certes remplie (bien-être économique et prévention des infractions), cela ne signifie pas pour autant que la proportionnalité est respectée. La fin ne justifie pas toujours les moyens.

En ce qui concerne la question de la nécessité, le texte est totalement disproportionné. Seules les données indispensables peuvent être enregistrées. L'enregistrement ne peut avoir lieu de manière massive ou permanente.

En outre, des garanties contre les abus doivent être mises en place et il s'impose de prévoir un contrôle indépendant, une notification et une possibilité de recours. Pour la consultation du PCC, seul le login est réglementé par la loi, ce qui n'est d'ailleurs pas prévu dans le cas du *money control*. Il n'est pas question d'un contrôle indépendant.

La conclusion sur la base de l'article 8 de la CEDH est que la Cour sera assassine à l'égard du texte à l'examen, sauf en ce qui concerne l'objectif légitime.

— Autres dispositions pertinentes de la CEDH

La ConvEDH contient aussi l'article 6, qui consacre le droit à un procès équitable. Or, lorsque des données issues du PCC sont utilisées dans des procédures fiscales ou pénales, il y a lieu de se demander si la personne visée par ladite procédure a bénéficié d'un procès équitable lorsqu'elle n'a pas été pas informée de la collecte des données utilisées à son encontre.

Dans l'affaire *Jalloh c. Allemagne* (2006), la CEDH a considéré que toute preuve obtenue en violation de l'article 8 (droit au respect de la vie privée) pouvait aussi porter atteinte à l'article 6 (droit à un procès équitable), *a fortiori* lorsque l'intéressé n'avait pas la possibilité de la contester.

Le fait qu'il sera difficile de contester la preuve compte tenu du degré de nébulosité de l'algorithme régissant l'exploration de données dans le PCC constitue déjà un problème fondamental. Le système *money control* pourrait donc porter atteinte à l'article 6 de la CEDH.

L'intervenant souligne par ailleurs que l'article 13 de la ConvEDH prévoit le droit à un recours effectif. Les États sont tenus de garantir ce droit, qui peut être invoqué en cas de violation des droits consacrés par la CEDH.

Het systeem van datamining in het CAP voorziet echter geen afzonderlijke procedure voor burgers om inzage te krijgen in raadplegingen, noch om de rechtmatigheid ervan te betwisten. De GBA heeft geen structurele toegang tot de logs en kan individuele raadplegingen niet automatisch verifiëren. Het Europees Hof heeft in de zaak *Klass e.a. tegen Duitsland* (1978) nochtans benadrukt dat toezicht alleen effectief is indien de controle onafhankelijk en voldoende geïnformeerd is. Men kan bijgevolg concluderen dat België theoretisch wel mogelijkheden voorziet, zoals vermeld in artikel 13 van het EVRM, maar niet de effectieve rechtsmiddelen die vereist zijn.

Verder wordt in artikel 14 van het EVRM het verbod op discriminatie vastgelegd. Hoewel het CAP en *money control* formeel op iedereen van toepassing zijn, kan indirecte discriminatie ontstaan als de algoritmen die worden toegepast systematisch bepaalde categorieën vaker aanduiden voor controle. Het kan bijvoorbeeld gaan over zelfstandigen of ondernemers of allerlei andere groepen. Dat was ook het probleem in Nederland, waar datamining leidde tot de toeslagenaffaire. In de SyRI-zaak werd nochtans beweerd dat er sprake was van menselijke controle, maar achteraf bleek dat slechts weinig voor te stellen. De menselijke tussenkomst in de Nederlandse casus was vergelijkbaar met de in het voorliggende amendement nr. 15 voorziene regeling. Mogelijk wordt artikel 14 van het EVRM – het verbod op discriminatie – bijgevolg ook geschonden.

Het Europees Hof erkende in de zaak *D.H. en anderen tegen Tsjechië* in 2007 dat statistische patronen van ongelijke behandeling ook onder artikel 14 kunnen vallen. Als *money control*-profielen systematisch een ongelijke uitwerking kennen, kan dit in de toekomst discriminatoire effecten opleveren.

— Samenvattende beoordeling

Samengevat hanteert de rechtspraak van het Europees Hof voor de Rechten van de Mens drie fundamentele principes voor de beoordeling van databanken en surveillance. Vooreerst het beginsel van proportionaliteit, dus geen algemene opslag zonder differentiatie. Ten tweede: transparantie en kennisgeving, waarbij burgers op zijn minst achteraf moeten kunnen vernemen dat zij onderwerp waren van toezicht. Ten derde: onafhankelijk toezicht, waarbij een rechterlijke of functioneel onafhankelijke instantie vooraf of tijdens de verwerking toezicht moet houden.

Le système d'exploration des données qui sera appliqué dans le PCC ne prévoira toutefois aucune procédure distincte permettant aux citoyens de prendre connaissance des consultations effectuées et d'en contester la légalité. En effet, l'APD n'a pas d'accès structurel aux journaux de consultations et ne peut pas non plus vérifier automatiquement les consultations individuelles. Dans l'affaire *Klass et autres c. Allemagne* (1978), la Cour européenne avait pourtant souligné que la surveillance n'était efficace qu'en cas de contrôle indépendant et suffisamment éclairé. On peut donc conclure que, s'il est vrai que la Belgique prévoit des possibilités de recours, telles que visées à l'article 13 de la CEDH, ces recours ne sont néanmoins pas effectifs.

Le membre poursuit en indiquant que l'article 14 de la CEDH interdit toute discrimination. Bien que le PCC et *money control* s'appliqueront formellement à chacun, une discrimination indirecte pourrait naître si les algorithmes utilisés désignent systématiquement plus souvent certaines catégories de personnes à des fins de contrôle. Songeons par exemple aux travailleurs indépendants ou aux entrepreneurs, ou à toutes sortes d'autres catégories de personnes. C'était aussi le problème aux Pays-Bas, où l'exploration des données a provoqué le scandale des allocations familiales. Dans l'affaire SyRI, il avait pourtant été affirmé qu'un contrôle humain avait lieu, mais il est apparu par la suite que celui-ci était très limité. L'intervention humaine prévue dans le cas néerlandais était comparable au système prévu dans l'amendement n° 15. Il se pourrait donc aussi que *money control* soit contraire à l'article 14 de la CEDH (interdiction de discrimination).

Dans l'affaire *D.H. et autres c. République tchèque* (2007), la CEDH a reconnu que les statistiques peuvent étayer l'existence d'une inégalité de traitement au sens de l'article 14. Si les algorithmes de *money control* opèrent systématiquement de manière discriminatoire, cela pourrait créer des discriminations à l'avenir.

— Résumé de l'évaluation

En résumé, la jurisprudence de la Cour européenne des droits de l'homme applique trois principes fondamentaux pour l'évaluation des banques de données et de la surveillance. Premièrement, le principe de proportionnalité, qui fait obstacle à tout stockage global sans différenciation. Deuxièmement, les principes de transparence et de notification, en vertu desquels les citoyens doivent à tout le moins être informés *a posteriori* qu'ils ont fait l'objet d'un contrôle. Troisièmement, le principe de contrôle indépendant, en vertu duquel une instance judiciaire ou fonctionnelle indépendante doit exercer un contrôle avant ou pendant le traitement des données.

Het Belgische CAP, en bij uitbreiding *money control*, voldoet nauwelijks aan de voorwaarden die het Europees Hof stelt. Misschien voldoet het deels aan de tweede bepaling (kennisgeving via logging), maar zeker niet aan de eerste en derde (proportionaliteit en onafhankelijk toezicht). De plannen van de minister zijn veel te ruim, de controle is te beperkt en de burgerrechten zijn uitermate zwak beschermd.

— *De Belgische context in het licht van de EVRM-normen*

België verdedigt het bestaande CAP als een instrument van financieel toezicht dat vergelijkbaar is met registers in andere EU-lidstaten. Toch verschilt de Belgische aanpak fundamenteel: in Duitsland en Oostenrijk is toegang enkel mogelijk na een rechterlijk bevel; in Nederland bestaat er een meldplicht en toezicht door de Autoriteit Persoonsgegevens. België daarentegen kent een structurele toegang voor de administratie, zonder rechterlijke toetsing.

— *De EHRM-lijn*

Volgens de criteria van het Europees Hof voor de Rechten van de Mens betekent dit dat België met *money control* de grenzen van artikel 8 van het EVRM zeker overschrijdt. Het Hof heeft in de afgelopen decennia een strenge lijn ontwikkeld ten aanzien van preventieve en systemische gegevensverzamelingen.

De spreker verwijst in dit verband nogmaals naar de zaken *Klass e.a. tegen Duitsland* (1978), waarin onafhankelijke toetsing vereist werd voor surveillance, *Amann tegen Zwitserland* (2000), waarin registratie op zich al een inmenging vormt en *Rotaru tegen Roemenië* (2000), waarin is geoordeeld dat een vage wet onvoldoende kwaliteit biedt. In de zaak *S. en Marper tegen het Verenigd Koninkrijk* (2008) oordeelde het Hof dat er geen algemene bewaring van gegevens mag zijn zonder noodzaak. In het arrest *Zakharov tegen Rusland* (2015) werd geoordeeld dat het bestaan van een systeem dat toegang verleent tot gegevens zelf al een schending van het Verdrag kan vormen. In de zaak *Big Brother Watch e.a. tegen het Verenigd Koninkrijk* (2021) stelde het Hof dat massale dataverwerking enkel aanvaardbaar is met strikte waarborgen. Op basis van deze rechtspraak ontwikkelde het Hof een Europees proportionaliteitsmodel, en België bevindt zich aan de uiterste rand daarvan.

Le PCC belge, et par extension *money control*, ne répond guère aux conditions fixées par la CEDH. Il satisfait peut-être en partie à la deuxième disposition (notification par journalisation), mais certainement pas à la première ni à la troisième (proportionnalité et contrôle indépendant). La portée des projets du ministre est beaucoup trop large, le contrôle sera trop limité et les droits des citoyens seront extrêmement mal protégés.

— *Le contexte belge à la lumière des normes de la CEDH*

La Belgique défend le PCC existant en arguant qu'il s'agit d'un instrument de surveillance financière comparable aux registres instaurés dans d'autres États membres de l'Union européenne. Toutefois, l'approche belge diffère fondamentalement. En effet, en Allemagne et en Autriche, l'accès à ces registres n'est possible qu'en vertu d'une injonction judiciaire, tandis qu'aux Pays-Bas, la loi prévoit une obligation de notification et un contrôle par l'Autorité chargée des données à caractère personnel. La Belgique, en revanche, accorde un accès structurel à l'administration, sans contrôle judiciaire.

— *Approche de la CEDH*

Si l'on examine les critères retenus par la Cour européenne des droits de l'homme, force est de constater que le système de *money control* belge dépasse indubitablement les limites de l'article 8 de la CEDH. La Cour a développé au cours des dernières décennies une approche stricte en matière de collecte préventive et systématique de données.

À cet égard, l'intervenant renvoie une nouvelle fois à l'affaire *Klass et autres c. l'Allemagne* (1978), dans laquelle un contrôle indépendant était requis pour les mesures de surveillance, à l'affaire *Amann c. la Suisse* (2000), dans laquelle la Cour a considéré que l'enregistrement en soi constituait déjà une ingérence, et à l'affaire *Rotaru c. la Roumanie* (2000), dans laquelle il a été jugé qu'une loi vague ne satisfaisait pas à l'exigence de qualité. Dans l'affaire *S. et Marper c. le Royaume-Uni* (2008), la Cour a estimé que la conservation générale de données ne pouvait pas avoir lieu sans nécessité. Dans l'arrêt *Zakharov c. la Russie* (2015), elle a jugé que l'existence même d'un système de consultation des données pouvait constituer une violation de la Convention. Dans l'affaire *Big Brother Watch et autres c. le Royaume-Uni* (2021), la Cour a indiqué que le traitement massif des données n'était acceptable qu'à condition de respecter des garanties strictes. Sur la base de cette jurisprudence, elle a développé un modèle européen de proportionnalité, et la Belgique se situe à l'extrémité de ce modèle.

De noodzakelijkheid in een democratische samenleving betekent volgens artikel 8, lid 2 van het EVRM dat er een dringende maatschappelijke behoefte (*“pressing social need”*) moet bestaan. De inmenging moet onontbeerlijk zijn voor het doel. Het systeem van *money control* is echter niet gebaseerd op empirisch bewijs dat de algemene registratie van alle rekeningen noodzakelijk is voor fiscale rechtvaardigheid. Het systeem is handig, maar niet noodzakelijk.

In de zaak *S. en Marper tegen het VK* (2008) maakte het Hof duidelijk dat efficiëntie voor de overheid geen voldoende rechtvaardiging vormt voor massale gegevensbewaring. Toch is dat precies het argument dat de minister gebruikt in zijn verantwoording.

Het EHRM is in dit opzicht glashelder: de doelstelling moet niet alleen nuttig zijn, maar vooral ook onontbeerlijk. Vanuit dat perspectief is *money control* een maatregel van structurele preventie, niet van noodzakelijkheid.

— *Koppeling met toekomstige datamining (money control)*

De koppeling met toekomstige datamining, waarbij algemene algoritmen patronen in het CAP analyseren en mogelijke fouten detecteren, verschuift het evenwicht nog verder. Volgens het EHRM impliceert profilering op basis van persoonlijke gegevens een verhoogde inmenging die enkel aanvaardbaar is bij strikte wettelijke afbakening, menselijke tussenkomst, onafhankelijk voorafgaand toezicht en duidelijke kennisgeving achteraf.

Zonder die waarborgen kwalificeert dergelijke profilering zich volgens het Hof in Straatsburg als een disproportionele inmenging. Toegepast op *money control* betekent dit ten eerste dat het algemene en ongedifferentieerde karakter strijdig is met de rechtspraak in de zaken *S. en Marper tegen het Verenigd Koninkrijk* en *Zakharov tegen Rusland*. Ten tweede wijst het ontbreken van voorafgaande rechterlijke toetsing op een tekort aan onafhankelijk toezicht. Ten derde ondermijnt het ontbreken van kennisgeving achteraf aan betrokkenen het recht op een effectief rechtsmiddel zoals voorzien in artikel 13 van het EVRM. Ten vierde vereist het hoge risico op vals positieve resultaten, eigen aan datamining, juist méér waarborgen en niet minder.

Zonder fundamentele hertekening van de wettelijke begrenzing per doeleinde, voorafgaande goedkeuring, notificatie achteraf, strikte bewaartermijnen en afdwingbare rechtsmiddelen is *money control* niet conform het EVRM.

La notion de nécessité dans une société démocratique signifie, selon l'article 8, paragraphe 2, de la CEDH, qu'il doit exister un besoin social impérieux (*“pressing social need”*). L'ingérence doit être indispensable à la réalisation de l'objectif poursuivi. Or, le *money control* ne repose pas sur des preuves empiriques démontrant que l'enregistrement général de tous les comptes est nécessaire à la justice fiscale. Ce système est pratique, mais pas indispensable.

Dans l'affaire *S. et Marper c. le Royaume-Uni* (2008), la Cour a clairement indiqué que l'efficacité administrative ne justifiait pas à elle seule la conservation massive des données. Il s'agit pourtant précisément de l'argument avancé par le ministre.

La Cour est limpide à ce sujet: l'objectif doit non seulement être utile, mais surtout indispensable. Dans ce contexte, le *money control* constitue une mesure de prévention structurelle, et non une mesure nécessaire.

— *Lien avec le futur data mining (money control)*

Le lien avec le futur *data mining*, dans le cadre duquel des algorithmes généraux analyseront les modèles du PCC et détecteront d'éventuelles erreurs, accentue encore le déséquilibre. Selon la Cour européenne des droits de l'homme, le profilage fondé sur des données personnelles constitue une ingérence accrue, qui n'est acceptable que dans le cadre d'une délimitation juridique stricte et moyennant une intervention humaine et l'instauration d'une surveillance indépendante préalable et d'une notification claire *a posteriori*.

En l'absence de ces garanties, un tel profilage constitue, selon la Cour de Strasbourg, une ingérence disproportionnée. Appliqué au *money control*, cela signifie tout d'abord que son caractère général et indifférencié est contraire à la jurisprudence découlant des affaires *S. et Marper c. le Royaume-Uni* et *Zakharov c. la Russie*. Deuxièmement, l'absence de contrôle judiciaire préalable révèle que la surveillance indépendante est insuffisante. Troisièmement, le défaut de notification *a posteriori* aux personnes concernées porte atteinte au droit à un recours effectif prévu par l'article 13 de la CEDH. Quatrièmement, le risque élevé de faux positifs, inhérent au *data mining*, exige précisément la mise en place de plus de garanties, et non l'inverse.

À défaut de refonte fondamentale des limites légales pour chaque objectif et en l'absence d'autorisation préalable, de notification *a posteriori*, de délais de conservation stricts et de recours juridictionnels exécutoires, le *money control* n'est pas conforme à la CEDH.

— *Remediërvorststellen voor EVRM-conformiteit*

Sommige commissieleden zullen vragen of er dan geen constructief alternatief kan worden voorgelegd. Er bestaan inderdaad wel degelijk remediërende opties om *money control* in lijn te brengen met artikel 8 van het EVRM. Daartoe zijn minstens de volgende zes wetgevende ingrepen aangewezen.

Ten eerste is een precieze wettelijke finaliteit per toegangstype noodzakelijk, met limitatieve doeleinden, elk voorzien van een eigen wettelijke drempel. Daarnaast moet er een verbod komen op secundair hergebruik. Statistische verwerking mag uitsluitend gebeuren met geanonimiseerde (geen gepseudonimiseerde) data.

Een tweede mogelijke aanpassing betreft onafhankelijke voorafgaande controle. Er moet een rechterlijk bevel voorhanden zijn of een functioneel onafhankelijke autoriteit die elke nominatieve raadpleging vooraf goedkeurt. In spoedgevallen kan een verkorte procedure worden voorzien, met een *ex post* beoordeling binnen een strikt tijds kader.

Een derde ingreep houdt verband met de kennisgeving aan de betrokkene. Er moet een verplichte melding komen na afloop van het onderzoek, met wettelijk beperkte uitstel mogelijkheden. Bovendien moet er een recht op uitleg bestaan met betrekking tot de basis van de selectie, zeker wanneer profilering een rol heeft gespeeld.

De vierde voorgestelde wijziging betreft het hanteren van strikte bewaartermijnen, vastgelegd in de wet zelf. Er moet een maximale retentieperiode komen voor identiteitsgegevens, en een afzonderlijke termijn voor raadplegingslogs. Automatische en verifieerbare vernietiging moet wettelijk worden geregeld.

De vijfde aanpassing gaat over effectieve rechtsmiddelen en toezicht. Burgers moeten een individueel recht op toegang tot raadplegingslogs krijgen. Er is daarnaast een uitdrukkelijke nood aan bevoegdheden en middelen voor de Gegevensbeschermingsautoriteit, inclusief de mogelijkheid om periodieke audits uit te voeren op de toegang tot het CAP.

De zesde ingreep betreft profilering met een mensgerichte aanpak. Er moet een wettelijk verbod komen op volledig geautomatiseerde beslissingen en op algemene

— *Propositions visant à remédier au problème de conformité avec la CEDH*

D'aucuns pourraient se demander s'il n'existe pas d'alternative constructive. Le membre confirme que des solutions existent pour rendre le contrôle des flux financiers (*money control*) conforme à l'article 8 de la CEDH. Il s'indiquera de prendre au minimum six initiatives législatives à cette fin.

Premièrement, il conviendra de déterminer une finalité légale précise pour chaque type d'accès. Ces finalités devront être limitatives et chacune devra être assortie d'un seuil légal propre. Par ailleurs, toute réutilisation secondaire devra être interdite. Le traitement des données à des fins statistiques ne pourra être autorisé qu'à partir de données anonymisées (et non à partir de données pseudonymisées).

Une deuxième modification possible concerne l'instauration d'un contrôle préalable indépendant. Toute consultation nominative devra, au préalable, faire l'objet d'un mandat de justice ou être approuvée par une autorité fonctionnellement indépendante. Une procédure accélérée pourra être prévue pour les cas d'urgence; une évaluation *ex post* devra alors être réalisée dans un délai strict.

La troisième initiative législative concerne la notification à la personne concernée. Il faudra prévoir une notification obligatoire à l'issue du contrôle et des possibilités de report limitées par la loi. En outre, la personne concernée devra pouvoir invoquer le droit d'obtenir des explications sur le motif de la sélection, en particulier lorsque le profilage aura joué un rôle.

La quatrième modification proposée concerne l'application de délais de conservation stricts, inscrits dans la loi elle-même. Il conviendra de fixer une durée maximale de conservation des données d'identification et un délai distinct pour les journaux de consultation. La loi devra également encadrer la destruction automatique et vérifiable des données.

La cinquième modification concerne les voies de recours effectives et les contrôles. Les citoyens devront disposer d'un droit d'accès individuel aux journaux de consultation. Il est en outre manifestement nécessaire de doter l'Autorité de protection des données de compétences et de lui allouer des moyens à cet effet. Celle-ci devra notamment avoir la possibilité de procéder à des audits périodiques de l'accès au PCC.

La sixième mesure concerne le profilage centré sur l'individu. La législation devra interdire les décisions entièrement automatisées et le *data mining* général. Il

datamining. Verplichte *data protection impact assessments* en menselijke besluitvorming met dossiermotivering zijn noodzakelijk.

Deze zes waarborgen vertalen rechtstreeks de *end-to-end safeguards* uit de rechtspraak van het Europees Hof naar de context van *money control*.

— Conclusie

De heer Van Quickenborne besluit het tweede deel van zijn analyse over de Europese regelgeving met de vaststelling dat artikel 8 van het EVRM niet alleen de fysieke levenssfeer, maar ook het informatiedomein van de burger beschermt. Vanuit die optiek vormt *money control* een ernstige inmenging. Het systeem centraliseert financiële identiteitsgegevens van alle inwoners, en maakt deze toegankelijk voor meerdere autoriteiten. Dit kan enkel gerechtvaardigd worden indien de inmenging bij wet is voorzien, legitiem is en vooral noodzakelijk in een democratische samenleving, met adequate en effectieve waarborgen tegen willekeur.

De heer Van Quickenborne gaat vervolgens over tot de toetsing van *money control* aan het Handvest van de grondrechten van de Europese Unie (hierna “het EU-Handvest”).

Het EU-Handvest is afdwingbaar recht en geldt voor de EU-instellingen en de lidstaten wanneer zij het Europees Unierecht ten uitvoer brengen.

De AVG is Uniewetgeving. Nationale bepalingen die de AVG uitvoeren moeten worden getoetst aan dat Handvest.

Het lid benadrukt dat het EVRM en het EU-Handvest overlappende bepalingen hebben, maar verschillen in toepassingsgebied, toezicht, reikwijdte, juridisch karakter en beschermingsniveau.

Als de artikelen van beide instrumenten elkaar overlappen, bepaalt artikel 52, derde lid, van het EU-Handvest dat, voor zover rechten in het EU-Handvest overeenkomen met die van het EVRM, zij dezelfde betekenis en draagwijdte hebben als in het EVRM. Datzelfde artikel laat ook toe dat het EU-Handvest een ruimere bescherming biedt. Dat is vooral het geval bij artikel 8 van het EU-Handvest dat een autonoom recht op gegevensbescherming invoert, iets wat in artikel 8 van het EVRM enkel impliciet wordt afgeleid.

conviendra également d'imposer la réalisation d'analyses d'impact relatives à la protection des données et la prise de décision humaine assortie d'une justification du dossier.

Ces six mesures transposeront directement les garanties (*end-to-end safeguards*) prévues dans la jurisprudence de la CEDH dans le contexte du contrôle des flux financiers.

— Conclusion

M. Van Quickenborne conclut le deuxième volet de son analyse de la réglementation européenne par le constat que l'article 8 de la CEDH protège non seulement la vie privée physique, mais aussi le domaine d'information du citoyen. Vu sous cet angle, le contrôle des flux financiers constitue une ingérence grave. Le système centralisera les données d'identification financières de tous les habitants et les mettra à la disposition de plusieurs autorités. Or, cet accès ne pourra se justifier que si l'ingérence est prévue par la loi, légitime et surtout nécessaire dans une société démocratique, et si des garanties adéquates et efficaces sont prévues contre l'arbitraire.

M. Van Quickenborne examine ensuite le *money control* à la lumière de la Charte des droits fondamentaux de l'Union européenne (Charte de l'UE ci-après).

La Charte de l'UE est de droit contraignant et s'applique aux institutions de l'Union européenne et aux États membres lorsqu'ils mettent en œuvre le droit de l'Union européenne.

Le RGPD étant un acte législatif de l'Union européenne, les dispositions nationales qui mettent en œuvre le RGPD doivent être évaluées à la lumière de cette Charte.

Le membre souligne que certaines dispositions de la CEDH et de la Charte de l'UE se recoupent, mais diffèrent en termes de champ d'application, de contrôle, de portée, de caractère juridique et de niveau de protection.

En cas de chevauchement entre les articles de ces deux instruments, l'article 52, paragraphe 3, de la Charte de l'UE prévoit que si cette Charte contient des droits correspondant à des droits garantis par la CEDH, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. De plus, cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue. C'est surtout le cas à l'article 8 de la Charte de l'UE, qui accorde à toute personne un droit à la protection des données à caractère personnel la concernant, droit qui ne peut être déduit qu'implicitement de l'article 8 de la CEDH.

De spreker overloopt vervolgens de drie bepalingen van het EU-Handvest die relevant zijn voor de beoordeling van het CAP en *money control*, namelijk artikelen 7, 8 en 47.

Artikel 7 gaat over het recht op eerbiediging van privé, familie- en gezinsleven. Artikel 8 betreft de bescherming van persoonsgegevens. Artikel 47 handelt over het recht op een doeltreffend rechtsmiddel en op een onpartijdig gerecht.

Het Hof van Justitie van de Europese Unie (hierna “het Hof van Justitie” of “het Hof”) heeft in de afgelopen jaren deze principes uitgelegd in arresten die de contouren van de privacybescherming binnen de EU bepalen. Het lid licht vijf arresten toe.

In het arrest *Digital Rights Ireland Ltd.* (C-293/12) vernietigde het Hof de EU-Richtlijn Gegevensbewaring wegens schending van artikelen 7 en 8 van het EU-Handvest. Het Hof oordeelde dat algemene en ongedifferentieerde opslag van gegevens over alle burgers in strijd was met het proportionaliteitsbeginsel en dat de maatregel niet beperkt was tot wat strikt noodzakelijk is. Volgens het lid valt *money control* onder deze redenering.

In de arresten *Schrems I* (C-362/14) en *Schrems II* (C-311/18), over internationale doorgiften naar de Verenigde Staten, bevestigt het Hof van Justitie dat de gegevensbescherming een fundamenteel recht is met een eigen inhoud. Dit impliceert dat: (1) toegang door overheidsautoriteiten duidelijk begrensd en controleerbaar moet zijn, (2) burgers effectieve rechtsmiddelen moeten hebben tegen misbruik, en (3) buitenlandse wetgeving de essentie van de artikelen 7 en 8 van het EU-Handvest niet mag uithollen. Toegepast op *money control* blijkt dat het systeem geen effectieve rechtsmiddelen, kennisgeving of controle biedt en daarom niet doeltreffend is in de zin van het Handvest.

In het derde arrest *Tele2 Sverige AB* (C-203/15 en C-698/15) breidde het Hof van Justitie de principes van *Digital Rights Ireland Ltd.* uit en stelde dat algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens strijdig is met het EU-Handvest. Het Hof van Justitie stelde dat strikte waarborgen noodzakelijk zijn: (1) opslag mag alleen gericht zijn op personen of situaties met een verband met criminaliteit; (2) de toegang moet voorafgegaan worden door toestemming van een rechter of onafhankelijke instantie; (3) de gegevens moeten binnen een korte termijn worden vernietigd; (4) betrokkenen moeten op de hoogte worden gebracht, tenzij dat tijdelijk onmogelijk is.

L'intervenant parcourt ensuite les trois dispositions de la Charte de l'UE pertinentes pour l'évaluation du PCC et du *money control*, à savoir ses articles 7, 8 et 47.

L'article 7 porte sur le droit au respect de la vie privée et familiale et l'article 8 sur la protection des données à caractère personnel. Quant à l'article 47, il concerne le droit à un recours effectif et à accéder à un tribunal impartial.

Ces dernières années, la Cour de justice de l'Union européenne (“la Cour” ci-après) a interprété ces principes dans plusieurs arrêts qui établissent les contours de la protection de la vie privée au sein de l'Union européenne. Le membre commente cinq de ces arrêts.

L'arrêt *Digital Rights Ireland Ltd.* (C-293/12) de la Cour a invalidé la directive UE sur la conservation de données au motif qu'elle violait les articles 7 et 8 de la Charte de l'UE. La Cour a estimé que le stockage général et indifférencié de données relatives à tous les citoyens était contraire au principe de proportionnalité et que cette mesure n'était pas limitée à ce qui était strictement nécessaire. D'après le membre, ce raisonnement s'applique également au *money control*.

Dans les arrêts *Schrems I* (C-362/14) et *Schrems II* (C-311/18), portant sur les transferts internationaux vers les États-Unis, la Cour de justice confirme que la protection des données est un droit fondamental emportant son propre contenu. Cela implique que: (1) l'accès à ces données par les autorités publiques doit être clairement défini et vérifiable, (2) les citoyens doivent disposer de moyens de recours efficaces contre les abus et (3) la législation étrangère ne peut éroder l'essence des articles 7 et 8 de la Charte de l'UE. Si l'on applique ces principes à la législation *money control*, il apparaît que le système n'apporte pas de moyens de recours efficace, de méthode de notification ou de contrôle et n'est, par conséquent, pas efficace au sens de la Charte.

Dans le troisième arrêt *Tele2 Sverige AB* (C-203/15 et C-698/15), la Cour de justice a étendu les principes du *Digital Rights Ireland Ltd.* et a indiqué que la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation était en contradiction avec la Charte de l'UE. La Cour de justice a établi que des garanties strictes étaient nécessaires: (1) le stockage ne peut concerner que des personnes ou des situations présentant un lien avec la criminalité; (2) l'accès doit s'appuyer sur l'autorisation d'un juge ou d'une instance indépendante; (3) les données doivent être supprimées à court terme; (4) les intéressés doivent être avertis du traitement, sauf si cela est provisoirement impossible.

Toegepast op *money control* blijkt dat er geen rechterlijke goedkeuring, geen kennisgeving, of beperking in tijd of doelgroep is. Het zou dus volgens deze logica ook onverzoenbaar zijn met artikelen 7 en 8 van het EU-Handvest.

In het arrest *La Quadrature du Net e.a.* (C-511/18) bevestigde het Hof van Justitie dat het Unierecht zich verzet tegen algemene en ongedifferentieerde bewaring van persoonsgegevens, ook wanneer de nationale wetgever zich beroept op nationale veiligheid of criminaliteitsbestrijding. Het Hof van Justitie erkende in dat arrest enkele uitzonderingen: (1) tijdelijke bewaring bij concrete en ernstige bedreiging; (2) gerichte bewaring van specifieke categorieën personen; (3) uitzonderlijke omstandigheden met voorafgaande rechterlijke goedkeuring.

De overwegingen van het Hof van Justitie gelden niet alleen voor telecommunicatie, maar voor alle vormen van preventieve massaverzameling van persoonsgegevens.

Money control beoogt permanente en algemene opslag zonder individuele selectiecriteria. Volgens de redenering van bovengenoemd arrest is dit systeem structureel onverenigbaar met het EU-Handvest.

Het vijfde arrest *Ministerio Fiscal* (C-207/16) is belangrijk omdat het Hof van Justitie verduidelijkte dat de toegang tot persoonsgegevens door overheden alleen is toegestaan wanneer de inmenging voldoende ernstig wordt gerechtvaardigd door het nagestreefde doel. Zelfs beperkte toegang vereist precieze regels. *Money control* voorziet evenwel niet in zo'n precisie.

Indien in 2026 een hoorzitting over dit onderwerp plaatsvindt, stelt de spreker voor om de conformiteit van *money control* met de Europese regels te onderzoeken.

Artikelen 7 en 8 van het EU-Handvest leggen een dubbele bescherming op: privacy en gegevensbescherming. Dit betekent dat maatregelen zoals *money control* twee toetsingen moeten doorstaan: (1) is de inmenging in het privéleven gerechtvaardigd?; (2) wordt de verwerking van persoonsgegevens uitgevoerd in overeenstemming met de beginselen van artikel 8?

Artikel 7 van het EU-Handvest biedt dezelfde bescherming als artikel 8, maar het Hof van Justitie heeft het strikter geïnterpreteerd. Elke vorm van systematische opslag of toegang tot individuele noodzaak vormt een

Par analogie, la législation *money control* ne s'appuie pas sur une approbation judiciaire quelle qu'elle soit, n'implique pas de notification, n'est pas assortie d'une limitation dans le temps et ne concerne pas un groupe cible défini. Dans cette logique, elle est donc inconciliable avec les articles 7 et 8 de la Charte de l'UE.

Dans l'arrêt *La Quadrature du Net e.a.* (C-511/18), la Cour a confirmé que le droit de l'Union s'opposait à une conservation généralisée et indifférenciée des données à caractère personnel, même lorsque le législateur national invoque la sécurité nationale ou la lutte contre la criminalité. Dans cet arrêt, la Cour a toutefois reconnu quelques exceptions: (1) la conservation transitoire en cas de menace concrète et grave; (2) la conservation ciblée portant sur des catégories spécifiques de personnes; (3) la conservation en cas de circonstances exceptionnelles avec approbation judiciaire préalable.

Les considérations de la Cour de justice ne s'appliquent pas uniquement aux télécommunications, mais également à toutes les formes de collectes généralisées et préventives de données à caractère personnel.

La législation *money control* envisage un stockage permanent et généralisé, sans critère de sélection individuelle. Si l'on s'en tient au raisonnement de l'arrêt précité, ce système est structurellement incompatible avec la Charte de l'UE.

Le cinquième arrêt *Ministerio Fiscal* (C-207/16) est important parce que la Cour de justice y a précisé que l'accès des pouvoirs publics aux données à caractère personnel n'est autorisé que lorsque cette ingérence est suffisamment grave pour être justifiée par l'objectif poursuivi. Même un accès restreint nécessite des règles précises. Or, *money control* n'en prévoit pas.

Dans l'hypothèse où une audition à ce sujet serait organisée en 2026, l'intervenant propose d'examiner la conformité de *money control* aux règles européennes.

Les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne garantissent une double protection: la protection de la vie privée et la protection des données. Autrement dit, des mesures comme *money control* ne peuvent être autorisées qu'en cas de réponses affirmatives aux deux questions suivantes: (1) l'ingérence dans la vie privée est-elle justifiée? (2) le traitement des données à caractère personnel est-il mis en œuvre dans le respect des principes fixés à l'article 8?

L'article 7 de la Charte précitée offre la même protection que l'article 8, mais la Cour de justice l'a interprété de manière plus stricte. Toute forme de stockage ou d'accès systématique à des fins individuelles constitue

ernstige inmenging. De inmenging moet strikt worden afgebakend in tijd, doel en doelgroep. *Money control* schendt die principes, meent het Kamerlid. Het registreert iedereen voor onbepaalde duur en voor meerdere doeleinden.

Artikel 8 van het EU-Handvest vereist dat persoonsgegevens eerlijk worden verwerkt, voor specifieke doeleinden worden verzameld, enkel op een wettelijke grondslag en onder het toezicht van een onafhankelijke autoriteit. *Money control* faalt op minstens drie punten: de doeleinden zijn te breed, de toegang gebeurt zonder voorafgaande onafhankelijke controle en het recht op toegang en correctie is structureel en in strijd met leden 2 en 3 van artikel 8.

Overeenkomstig artikel 47 van het EU-Handvest is het recht op een doeltreffend rechtsmiddel een fundamenteel beginsel van de rechtstaat. In de zaken *Schrems II* en *La Quadrature du Net* heeft het Hof van Justitie geoordeeld dat personen in de praktijk moeten kunnen nagaan hoeveel gegevens zijn verwerkt, door wie en waarom. *Money control* voorziet echter geen kennisgeving bij raadpleging, geen procedure om raadplegingen te betwisten of transparantie over loggegevens. De burger beschikt dus niet over een doeltreffend rechtsmiddel in de zin van artikel 47 van het EU-Handvest. De GBA kan wel adviezen verlenen, maar heeft geen toegang tot individuele raadplegingslogs en kan slechts ex post optreden.

Artikel 52, eerste alinea, van het EU-Handvest bepaalt dat beperkingen op de uitoefening van grondrechten slechts zijn toegestaan indien ze (1) bij wet worden vastgesteld, (2) de wezenlijke inhoud van het recht eerbiedigen, (3) noodzakelijk en evenredig zijn en (4) een doel van algemeen belang nastreven. Volgens het lid voldoet *money control* niet aan de laatste drie voorwaarden.

De heer Van Quickenborne gaat dan over tot de vergelijking met de unierechtelijke proportionaliteitsnorm.

Het Hof van Justitie hanteert in privacyzaken een strenge, driedelige proportionaliteitstoets. Daarbij wordt gekeken naar de geschiktheid, de noodzakelijkheid en de evenredigheid in enge zin van de maatregel. Bij beoordeling van *money control* kan worden gesteld dat het geschikt is. Het vergemakkelijkt immers fraude-detectie. Het is echter niet noodzakelijk want gerichte registers of verantwoorde opvragingen volstaan. Het is evenmin evenredig want 100 % van de bevolking wordt

une ingérence grave. Cette ingérence doit être strictement limitée dans le temps, tout comme son objectif et le groupe-cible qu'elle concerne. Le membre estime que *money control* viole ces principes, dès lors que ce système enregistrera des informations sur tout un chacun pour une durée indéterminée et en vue de poursuivre plusieurs finalités.

L'article 8 de la Charte précitée impose que les données à caractère personnel soient traitées loyalement, collectées à des fins déterminées, uniquement en vertu d'un fondement légal et sous le contrôle d'une autorité indépendante. Sur ce plan, *money control* pêche au moins à trois égards: ses finalités sont trop larges, l'accès aux données se fera sans contrôle préalable indépendant et les droits d'accès et de rectification seront structurels et contraires aux alinéas 2 et 3 de l'article 8 précité.

En application de l'article 47 de la Charte précitée, le droit à un recours effectif constitue un principe fondamental de l'état de droit. Dans les affaires *Schrems II* et *La Quadrature du Net*, la Cour de justice a considéré que les personnes devaient en pratique pouvoir vérifier combien de leurs données ont été traitées, par qui et dans quel but. *Money control* ne prévoit toutefois aucune notification en cas de consultation, aucune procédure permettant de contester les consultations, ni aucune transparence concernant les fichiers journaux. Le citoyen ne disposera donc pas d'un recours effectif au sens de l'article 47 précité. S'il est vrai que l'APD peut rendre des avis, elle n'a néanmoins pas accès aux journaux de consultations individuels et ne peut agir qu'*a posteriori*.

L'article 52, alinéa 1^{er}, de la Charte précitée dispose qu'une limitation de l'exercice de droits fondamentaux n'est permise que si cette limitation (1) est prévue par la loi, (2) respecte le contenu essentiel de ces droits, (3) est nécessaire et proportionnée et (4) poursuit un objectif d'intérêt général. Le membre estime cependant que *money control* ne remplira pas les trois dernières conditions énoncées.

M. Van Quickenborne évoque ensuite la comparaison avec la norme de proportionnalité prévue par le droit européen.

Dans les affaires relatives au respect de la vie privée, la Cour de justice procède à un contrôle de proportionnalité strict en trois volets. Elle examine le caractère approprié de la mesure, sa nécessité et sa proportionnalité au sens strict du terme. L'examen du dispositif *money control* permet d'établir que ce dispositif sera approprié, dès lors qu'il facilitera la détection des fraudes. Cependant, il ne sera pas nécessaire, car des registres ciblés ou des consultations justifiées suffisent à cette fin. Il ne sera

geraakt voor een probleem dat slechts een fractie van de burgers betreft.

Het lid analyseert vervolgens de rol van de GBA in het licht van artikel 8, derde lid, van het EU-Handvest. Dat artikel schrijft voor dat de naleving van de gegevensbeschermingsregels wordt gecontroleerd door een onafhankelijke autoriteit. Artikel 8 is in nauwe samenhang te lezen met artikel 51 van de AVG.

De GBA vervult de rol van de autoriteit beschreven in artikel 8, derde lid, van het EU-Handvest, maar het ontvangt geen automatische meldingen van raadpleging, het heeft geen systematische toegang tot de CAP-logs en het oefent enkel ex post toezicht uit.

In het arrest van de Europese Commissie tegen Republiek Oostenrijk (C-614/10) heeft het Hof van Justitie geoordeeld dat functionele en organisatorische onafhankelijkheid absoluut is. Als een toezichthouder onvoldoende middelen of informatie heeft om op te treden, dan is die onafhankelijkheid feitelijk uitgehold. Dus voldoet ook hier *money control* niet aan de Handvestnorm, aldus de spreker.

Het Hof van Justitie onderscheidt in zijn arrest jurisprudentie tussen beperkingen die binnen de grenzen van de proportionaliteit vallen en maatregelen die de essentie van het recht aantasten. Volgens het Hof tast een maatregel de essentie van het recht aan wanneer de betrokkenen elke effectieve controle over gegevens wordt ontnomen en als het risico wordt gecreëerd op permanente systematische monitoring. Volgens de spreker maakt *money control* zich daaraan schuldig.

Het Kamerlid behandelt dan de gevolgen van een schending van het EU-Handvest.

Indien een nationale wet in strijd is met het EU-Handvest, dan kan een nationale rechter die bepalen buiten toepassing laten en kunnen de burgers zich rechtstreeks beroepen op het EU-Handvest bij een nationale rechtbank.

Het Hof van Justitie heeft herhaaldelijk bevestigd dat nationale wetten die algemene en ongedifferentieerde gegevensbewaring invoeren ongeldig zijn binnen de sfeer van het Unierecht. Daaruit volgt dat *money control* rechtstreeks aan het EU-Handvest kan worden getoetst en potentieel buiten toepassing kan worden verklaard.

Money control bevindt zich op het kruispunt van drie spanningsvelden: de nationale soevereiniteit in fiscaliteit,

pas non plus proportionné dans la mesure où il vise la population dans son ensemble, alors que le problème qu'il vise à éliminer ne concerne qu'une fraction des citoyens.

Le membre poursuit en analysant le rôle de l'APD à la lumière de l'article 8, alinéa 3, de la Charte européenne des droits fondamentaux, selon lequel il revient à une autorité indépendante de contrôler le respect des règles relatives à la protection des données. Cet article 8 doit être lu en étroite corrélation avec l'article 51 du RGPD.

L'APD remplit le rôle de l'autorité prévue par l'article 8, alinéa 3, de la Charte précitée, mais elle ne reçoit pas de notifications automatiques de consultation, elle ne dispose pas d'un accès systématique aux fichiers journaux du PCC et elle n'exerce qu'un contrôle *a posteriori*.

Dans l'affaire opposant la Commission européenne à la République d'Autriche (C-614/10), la Cour de justice a considéré que l'indépendance fonctionnelle et organisationnelle était absolue. Si une autorité de contrôle dispose d'insuffisamment de moyens ou d'informations pour agir, son indépendance est sapée dans les faits. L'intervenant considère donc que, sur ce point, *money control* ne respecte pas non plus la Charte des droits fondamentaux de l'Union européenne.

Dans sa jurisprudence, la Cour de justice distingue les limitations qui restent dans les limites de la proportionnalité et les mesures qui portent atteinte à l'essence même du droit. Selon la Cour, une mesure porte atteinte à l'essence du droit lorsque les personnes concernées sont privées de tout contrôle effectif de leurs données et lorsqu'un risque de suivi systématique permanent apparaît. L'intervenant estime que ce sera le cas avec *money control*.

Le député examine ensuite les répercussions d'une violation de la Charte de l'UE.

Si une loi nationale est contraire à la Charte de l'UE, un juge national peut ne pas appliquer les dispositions de cette loi et les citoyens peuvent invoquer directement la Charte précitée devant un tribunal national.

La Cour de justice a confirmé à plusieurs reprises que les lois nationales qui instaurent une conservation générale et indifférenciée des données sont invalides dans le cadre du droit de l'Union. Il s'ensuit que *money control* peut être directement évalué à la lumière de la Charte de l'UE et potentiellement déclaré inapplicable.

Money control se trouve à la croisée de trois domaines conflictuels, à savoir la souveraineté nationale en matière

de Europese gegevensbescherming en de constitutionele rechtstatelijkheid binnen de EU.

Het EU-Handvest legt aan lidstaten ook op gevoelige domeinen als fiscaliteit de plicht op om de fundamentele rechten van de burgers te respecteren telkens wanneer zij Unierecht toepassen of uitvoeren. De combinatie van universele registratie, ongedifferentieerde bewaring, gebrek aan rechterlijke controle en afwezigheid van effectieve kennisgeving van rechtsmiddelen plaatst het systeem op gespannen voet met artikelen 7, 8, 47 en 52 van het EU-Handvest.

Hoewel de drie Europese rechtsniveaus (het Unierechtelijk kader van de AVG, de grondrechtelijke bescherming van het EU-handvest en het mensrechtelijke minimumkader van het EVRM) eigen waarborgen en terminologieën hanteren, dienen ze één fundamenteel uitgangspunt: de overheid mag enkel persoonsgegevens verzamelen, bewaren of gebruiken wanneer dat noodzakelijk, proportioneel, wettelijk en controleerbaar is in een democratische rechtstaat. Met de geplande uitbreiding via *money control* wil de overheid datamining en risicoprofilering toepassen om potentiële fraude te detecteren. Deze evolutie maakt van het CAP niet enkel een administratief register, maar een permanent financieel *surveillance* systeem.

De toetsing aan de drie juridische kaders leidt, elk via een eigen benadering, tot eenzelfde conclusie: er is sprake van een structurele disbalans. *Money control* kan in geen enkel Europees rechtskader worden gehandhaafd. Alles wijst op een structureel gebrek aan noodzakelijkheid, transparantie en controle.

Money control zou een nieuwe dimensie toevoegen aan het CAP, namelijk de automatische analyse van de CAP-gegevens, algoritmische detectie van risicoprofielen en verplichte controle bij hoge score. Dit brengt het systeem rechtstreeks in het domein van artikel 22 van de AVG en artikel 8 van het EU-Handvest. Zonder substantiële menselijke toetsing of mogelijkheid tot betwisting zou *money control* leiden tot een volledige automatisering van fiscale verdenking. Dat is een stap verder dan louter registratie. Daarmee zou ons land evolueren van passieve gegevensbewaring naar actieve gegevensprofilering, wat in het Europees recht enkel toelaatbaar is onder uitzonderlijk strikte voorwaarden (zie SCHUFA-arrest C-634/21).

Money control is in strijd met de Europese rechtsorde op unionair, internationaal en nationaal vlak, besluit de spreker.

de fiscalité, la protection européenne des données et les principes constitutionnels relatifs à l'état de droit au sein de l'UE.

La Charte de l'UE impose également aux États membres, dans des domaines sensibles tels que la fiscalité, l'obligation de respecter les droits fondamentaux des citoyens chaque fois qu'ils appliquent ou mettent en œuvre le droit de l'Union. La combinaison d'un enregistrement universel, d'une conservation indifférenciée, d'un manque de contrôle judiciaire et d'une absence de notification effective des voies de recours rend le système incompatible avec les articles 7, 8, 47 et 52 de la Charte de l'UE.

Bien que les trois niveaux juridiques européens (le cadre juridique de l'UE du RGPD, la protection des droits fondamentaux de la Charte de l'UE et le cadre minimum des droits de l'homme de la CEDH) utilisent leurs propres garanties et terminologies, ils partagent un principe fondamental: les pouvoirs publics ne peuvent collecter, conserver ou utiliser des données à caractère personnel que lorsque cela est nécessaire, proportionné, légal et contrôlable dans un État de droit démocratique. Par le biais de l'extension prévue via *money control*, les pouvoirs publics souhaitent recourir au *data mining* et au profilage des risques afin de détecter les fraudes potentielles. Cette évolution fait du PCC non seulement un registre administratif, mais aussi un système permanent de surveillance financière.

L'évaluation à la lumière des trois cadres juridiques conduit, chacun selon sa propre approche, à la même conclusion: il est question d'un déséquilibre structurel. *Money control* ne peut être appliqué dans aucun cadre juridique européen. Tout indique un manque structurel de nécessité, de transparence et de contrôle.

Money control ajouterait une nouvelle dimension au PCC, à savoir l'analyse automatique de ses données, la détection algorithmique des profils à risque et le contrôle obligatoire en cas de score élevé. C'est pourquoi le système relève directement du domaine de l'article 22 du RGPD et de l'article 8 de la Charte de l'UE. Sans contrôle humain substantiel ni possibilité de contestation, *money control* conduirait à une automatisation complète des soupçons dans le domaine fiscal, ce qui va plus loin que le simple enregistrement. Notre pays passerait ainsi d'un stockage passif des données à leur profilage actif, ce qui n'est autorisé par le droit européen que dans des conditions extrêmement strictes (voir arrêt SCHUFA C-634/21).

L'intervenant conclut que *money control* est contraire à l'ordre juridique européen aux niveaux de l'Union, international et national.

De heer Van Quickenborne gaat vervolgens in op de Belgische rechtspraak.

Het Grondwettelijk Hof behandelde een beroep tot vernietiging tegen de uitbreiding van de toegang tot het CAP-register, ingevoerd bij de programmawet van 20 december 2020 (zie arrest 162/2022). Deze uitbreiding geeft de fiscus toegang tot periodieke saldi van bank- en betaalrekeningen en het totaalbedrag van bepaalde financiële contracten. De verzoekende partijen, een particulier en de non-profitorganisatie The Ministry of Privacy, stelden dat dit een schending vormt van het recht op bescherming van de persoonlijke levenssfeer, zoals gewaarborgd door artikel 22 van de Grondwet, artikel 8 EVRM en artikelen 7 en 8 van het EU-Handvest.

Het Grondwettelijk Hof onderzocht eerst de bestaande modaliteiten van het CAP, zoals ingevoerd in 2011 en uitgebreid in 2018. Het Hof oordeelde dat deze modaliteiten niet werden gewijzigd door de bepalingen van december 2020, waardoor dit deel van het beroep onontvankelijk was.

Het resterende geschil betrof de uitbreiding van de meldingsplicht tot saldi. Het Hof erkende dat het verzamelen en verwerken van deze gegevens een inmenging in het privéleven is, maar toetste dit aan drie voorwaarden: een voldoende precieze wettelijke basis, een dwingende maatschappelijke behoefte en evenredigheid met het nagestreefde doel. De eerste twee voorwaarden werden vervuld geacht, aangezien de uitbreiding kadert in de verhoging van fiscale transparantie en de bestrijding van belastingfraude, wat ook ten goede komt aan andere bevoegde instanties zoals het parket en de veiligheidsdiensten.

Opmerkelijk is dat het Hof zich nauwelijks kritisch toonde tegenover de door de wetgever aangehaalde doelstelling van de uitbreiding. Het lijkt zonder meer akkoord te gaan met de stelling dat belastingplichtigen vaak onwillig zijn om mee te werken aan fiscale onderzoeken. Daarmee gaat het Hof voorbij aan het feit dat er reeds bestaande procedures zijn om informatie op te vragen bij onwil. Dit roept vragen op over het impliciete wantrouwen tegenover burgers en financiële instellingen, dat contrasteert met het grote vertrouwen in de fiscale administratie. Dit vertrouwen is des te opvallender omdat de Geschillenkamer van de Gegevensbeschermingsautoriteit in haar beslissing van 4 juni 2021 (nr. 66/2021) heeft vastgesteld dat de fiscus zelfs niet beschikt over een interne procedure om een volledig overzicht te hebben van alle persoonsgegevens die hij verwerkt. Bovendien blijkt het CAP-register onvolledig, bijvoorbeeld voor

M. Van Quickenborne évoque ensuite la jurisprudence belge.

La Cour constitutionnelle a été saisie d'un recours en annulation contre l'élargissement de l'accès au registre PCC, introduit par la loi-programme du 20 décembre 2020 (voir arrêt 162/2022). Cet élargissement visait à permettre à l'administration fiscale d'accéder aux soldes périodiques des comptes bancaires et de paiement ainsi qu'au montant globalisé de certains contrats financiers. Les parties requérantes, un particulier et l'association sans but lucratif The Ministry of Privacy, ont avancé que l'élargissement visé constituait une violation du droit à la protection de la vie privée, tel que consacré par l'article 22 de la Constitution, l'article 8 de la CEDH et les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

La Cour constitutionnelle a d'abord examiné les modalités actuelles du PCC, telles qu'introduites en 2011 et élargies en 2018. Elle a estimé que ces modalités n'avaient pas été modifiées par les dispositions de décembre 2020, cette partie du recours étant dès lors irrecevable.

Le point resté litigieux visait l'élargissement de l'obligation de communiquer les soldes. La Cour a reconnu que la collecte et le traitement de ces données constituaient une ingérence dans le droit au respect de la vie privée, mais a confronté cette question à trois conditions: une base légale suffisamment précise, un besoin social impérieux et la proportionnalité à l'objectif poursuivi. Les deux premières conditions ont été jugées remplies, étant donné que l'élargissement s'inscrit dans le cadre de l'amélioration de la transparence fiscale et de la lutte contre la fraude fiscale, ce qui profite également à d'autres autorités compétentes telles que le parquet et les services de sécurité.

Force est de constater que la Cour ne s'est guère montrée critique à l'égard de l'objectif de l'élargissement invoqué par le législateur. Elle semble tout à fait d'accord avec l'affirmation selon laquelle les contribuables sont souvent réticents à coopérer aux enquêtes fiscales. Ce faisant, la Cour ignore le fait qu'il existe déjà des procédures permettant de réclamer des informations en cas de réticence. Cette position soulève des questions quant à la méfiance implicite à l'égard des citoyens et des établissements financiers, qui contraste avec la grande confiance accordée à l'administration fiscale. Cette confiance est d'autant plus surprenante que la Chambre contentieuse de l'Autorité de protection des données a constaté, dans sa décision du 4 juin 2021 (n° 66/2021), que l'administration fiscale ne dispose même pas d'une procédure interne permettant d'avoir un aperçu complet de toutes les données à caractère

buitenlandse rekeningen, wat de effectiviteit van de maatregel in vraag stelt.

Bij de evenredigheidstoets stelde het Hof dat de uitbreiding proportioneel is, ondanks het bestaan van alternatieve, zij het minder efficiënte, werkwijzen. Het Hof benadrukte dat de wetgever niet verplicht was om een minimumdrempel voor saldi in te voeren, omdat een laag saldo niet uitsluit dat er veel transacties plaatsvinden. Criminele organisaties werken vaak met talrijke kleine verrichtingen, waardoor een drempel de effectiviteit van de maatregel zou ondermijnen. De raadpleging van het CAP blijft strikt omkaderd: fiscale ambtenaren mogen enkel consulteren bij aanwijzingen van belastingontduiking en moeten de belastingplichtige informeren. Deze waarborgen moeten willekeurige inmenging voorkomen.

De spreker merkt echter op dat het Hof de proportionaliteitstoets beperkt heeft uitgevoerd. Het arrest gaat nauwelijks in op de vraag of deze verregaande centralisatie van gegevens noodzakelijk is, gelet op het bestaan van alternatieve procedures en het feit dat de efficiëntiewinst mogelijk beperkt is. Ook blijft onduidelijk of de uitbreiding in verhouding staat tot het doel, aangezien veel meer gegevens worden verzameld dan strikt nodig voor fraudeonderzoek.

Het beroep tot vernietiging van de artikelen 18 tot en met 22 van de programmawet werd verworpen. De CAP-wetgeving blijft dus in stand, maar het arrest laat ruimte voor debat.

De spreker vraagt zich af of ook het Hof van Cassatie zich over het CAP-vraagstuk heeft gebogen.

De heer Vincent Van Quickenborne (Open Vld) verwijst naar verschillende arresten van het Hof van Justitie van de Europese Unie, met name het *Digital Rights Ireland*-arrest (C-293/12), teneinde te benadrukken dat elke nationale wetgeving die een algemene en ongedifferentieerde verplichting oplegt om verkeers- en locatiegegevens te bewaren, in combinatie met geautomatiseerde analyses, reeltimetoeegang of massale bewaring, onverenigbaar is met het recht van de Europese Unie.

De spreker merkt evenwel op dat men er op basis van die rechtspraak van kan uitgaan dat België nog steeds de mogelijkheid heeft om gegevens te bewaren en tegelijk controles uit te voeren, naar het voorbeeld van andere Europese landen. Hij wijst erop dat de relatie tussen fiscale transparantie en bescherming van privacy een

personeel d'une personne concernée qu'elle traite. De plus, le registre du PCC s'avère incomplet, par exemple pour les comptes étrangers, ce qui remet en question l'efficacité de la mesure.

Dans le cadre du contrôle de proportionnalité, la Cour a estimé que l'élargissement était proportionné, malgré l'existence d'autres méthodes, certes moins efficaces. La Cour a souligné que le législateur n'était pas tenu d'introduire un seuil minimal pour les soldes, car un solde faible n'exclut pas la possibilité que de nombreuses transactions aient lieu. Les organisations criminelles effectuent souvent un grand nombre de transactions d'un montant relativement faible, de sorte qu'un seuil compromettrait l'efficacité de la mesure. La consultation du PCC demeure strictement encadrée: les fonctionnaires de l'administration fiscale ne peuvent procéder à une consultation que s'il existe des indices de fraude fiscale et doivent en informer le contribuable. Ces garanties visent à prévenir toute ingérence arbitraire.

L'intervenant fait toutefois observer que la Cour n'a procédé qu'à un contrôle de proportionnalité limité. L'arrêt ne se penche guère sur la question de savoir si cette centralisation accrue des données est nécessaire, compte tenu de l'existence de procédures alternatives et du fait que le gain d'efficacité est peut-être limité. Il reste également difficile de déterminer si l'élargissement est proportionné à l'objectif, étant donné que les données collectées dépassent largement celles qui sont strictement nécessaires à la recherche de fraudes.

Le recours en annulation des articles 18 à 22 de la loi-programme a été rejeté. La législation PCC reste donc en vigueur, mais l'arrêt ouvre la porte au débat.

L'intervenant se demande si la Cour de cassation s'est également penchée sur la question du PCC.

M. Vincent Van Quickenborne (Open Vld) fait référence à plusieurs arrêts rendus par la Cour de justice de l'Union européenne, notamment l'arrêt *Digital Rights Ireland* (C-293/12), afin de souligner que toute législation nationale imposant une obligation générale et indifférenciée de conservation des données de trafic et de localisation, associée à des analyses automatisées, un accès en temps réel ou une conservation massive, est incompatible avec le droit de l'Union.

Partant de cette jurisprudence, l'orateur observe que l'on pourrait toutefois partir du principe que la Belgique pourrait encore conserver des données, tout en effectuant des contrôles, à l'instar d'autres pays européens. Il précise que la relation entre la transparence fiscale et la protection de la vie privée constitue l'un des exercices

van de meest delicate evenwichtsoefeningen is binnen het Europese rechtssysteem. Die spanning vloeit voort uit een dubbele eis. Enerzijds moeten er doeltreffende instrumenten worden uitgewerkt om belastingfraude, belastingontduiking en witwassen van geld te bestrijden; anderzijds moet de eerbiediging van de grondrechten worden gewaarborgd, in het bijzonder het recht op gegevensbescherming, dat is vastgelegd in artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en in de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie.

Het lid is daarom van mening dat een evenwicht moet worden gevonden tussen fraudebestrijding en eerbiediging van de in de Europese verdragen en het Handvest vastgelegde rechten. De spreker benadrukt dat dit nu net de complexiteit van een democratie is: veiligheid garanderen en tegelijk de vrijheden respecteren. Het Europese kader biedt elke lidstaat de mogelijkheid zijn eigen model uit te werken met betrekking tot de toegang tot bankinformatie door overheidsinstanties. In die context is het volgens de spreker belangrijk de nationale praktijken te onderzoeken. Hij vergelijkt België daarom met vijf Europese landen die een strikt gegevensbeschermingsbeleid hanteren: Zweden, Finland, Oostenrijk, Duitsland en Nederland.

Om te beginnen merkt het lid op dat de door België nagestreefde doelstellingen vergelijkbaar zijn met die van de voormelde vijf lidstaten, waar eveneens belastingfraudeproblemen blijven bestaan. De heer Van Quickenborne wijst er evenwel op dat de juridische structuren verschillen en dat het beschermingsniveau van de grondrechten sterk uiteenloopt. Hij stelt dat België sinds 2011 beschikt over een centraal aanspreekpunt bij de Nationale Bank, waar de identificatiegegevens van banken, betaalrekeningen en financiële contracten worden gecentraliseerd. De heer Van Quickenborne herinnert eraan dat minister Jambon onlangs aankondigde dat hij dat systeem wil uitbreiden naar de controle op geldstromen. Om die ontwikkeling in perspectief te plaatsen bespreekt de spreker de mechanismen die de voormelde vijf Europese staten hanteren om hetzelfde probleem aan te pakken.

De heer Van Quickenborne heeft het om te beginnen over Duitsland, waar een regeling geldt die de banken ertoe verplicht de identificatiegegevens van de rekening in een intern register bij te houden, met uitzondering van de naam, het adres, het rekeningnummer en de data van opening en afsluiting. De spreker licht toe dat die regeling fungeert als een technische brug tussen de banken en de bevoegde overheidsinstanties, wat een gedecentraliseerde aanpak weerspiegelt: er is geen centrale gegevensbank die door de Staat wordt bijgehouden.

les plus délicats au sein de l'ordre juridique européen. Selon l'orateur, cette tension implique une double exigence: d'une part, développer des instruments efficaces pour lutter contre la fraude fiscale, l'évasion et le blanchiment d'argent; d'autre part, garantir le respect des droits fondamentaux, en particulier le droit à la protection des données, consacré par l'article 8 de la Convention européenne des droits de l'Homme ainsi que par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

Le député estime dès lors qu'il est nécessaire de trouver un équilibre entre la lutte contre la fraude et le respect des droits inscrits dans les traités européens et la Charte. Il souligne qu'il s'agit là de toute la complexité d'une démocratie: assurer la sécurité tout en respectant les libertés. Selon lui, le cadre européen permet à chaque État membre de développer son propre modèle d'accès aux informations bancaires par les autorités publiques. Dans ce cadre, l'orateur souligne l'intérêt d'examiner les pratiques nationales et compare la Belgique avec cinq pays européens qui adoptent une politique stricte en matière de protection des données: la Suède, la Finlande, l'Autriche, l'Allemagne et les Pays-Bas.

D'emblée, le député constate que les objectifs poursuivis par la Belgique sont comparables à ceux de ces cinq États membres, où subsistent également des problèmes liés à la fraude fiscale. Toutefois, il relève que les structures juridiques diffèrent et que le niveau de protection des droits fondamentaux varie considérablement. Selon l'orateur, la Belgique dispose, depuis 2011, d'un point de contact central auprès de la Banque nationale, qui centralise les données d'identification des banques, des comptes de paiement et des contrats financiers. M. Van Quickenborne rappelle que le ministre Jambon a récemment annoncé son intention d'étendre ce dispositif au contrôle des flux financiers. Pour mettre cette évolution en perspective, l'orateur présente les mécanismes adoptés par les cinq autres États européens précités pour traiter la même problématique.

Pour commencer, M. Van Quickenborne aborde le cas de l'Allemagne: ce pays dispose d'un système qui impose aux banques de conserver, dans un registre interne, les informations d'identification des comptes, à l'exception du nom, de l'adresse, du numéro de compte ainsi que des dates d'ouverture et de clôture. L'orateur précise que ce mécanisme fonctionne comme une passerelle technique entre les banques et les autorités publiques compétentes, ce qui traduit une logique de décentralisation: il n'existe aucune base de données centrale détenue par l'État.

Ook wijst het lid erop dat het Duitse grondwettelijk hof heeft geoordeeld dat de regeling verenigbaar is met het informatieel zelfbeschikkingsrecht, op voorwaarde dat ze strikt individueel blijft en wordt onderworpen aan onafhankelijk toezicht. De heer Van Quickenborne concludeert daarom dat Duitsland geen gebruik maakt van datamining of geautomatiseerde risicoselectie, aangezien elk verzoek een menselijke beslissing en een motivering vereist. Het Duitse model wordt aldus beschouwd als de regeling met het meeste respect voor de grondrechten in heel Europa en als een referentie op het vlak van doeltreffendheid.

De spreker vervolgt met het voorbeeld van Oostenrijk, dat over een soortgelijke regeling beschikt als Duitsland, zij het met een belangrijk verschil: de gegevens worden gecentraliseerd bij de Oostenrijkse Nationale Bank. In de praktijk moet elke bank dagelijks de identificatiegegevens van haar klanten naar dat register doorsturen. De Nationale Bank beheert dat register als neutrale technische beheerder en heeft niet het recht om de gegevens voor analysedoeleinden te gebruiken. Voorts benadrukt de spreker dat datamining in Oostenrijk bij wet verboden is: de gegevens mogen alleen voor een wettelijk bepaald doel worden gebruikt en mogen niet worden verwerkt voor profileringsdoeleinden.

Wat Nederland betreft, stipt de heer Van Quickenborne aan dat het land geen gecentraliseerd bankregister heeft, maar werkt met een netwerk van onderling verbonden informatiesystemen. De spreker verduidelijkt dat bepaalde instanties, zoals de Nederlandse belastingdienst, voor concrete dossiers elektronische toegang hebben tot de bankgegevens. De banken hebben dan weer een wettelijke meldingsplicht. Er bestaat ook een register van daadwerkelijke begunstigen. De spreker voegt eraan toe dat de rechtsgrondslag is vastgelegd in verschillende wetteksten, waarin wordt bepaald dat de belastingdienst slechts algemene gegevensanalyses mag uitvoeren op de bankgegevens van de burgers. Er bestaan wel risicoselectiesystemen binnen de belastingdienst, maar die zijn uitsluitend van toepassing op de belastinggegevens en niet op de bankgegevens. Ten slotte benadrukt het lid dat de Nederlandse gegevensbeschermingsautoriteit toeziet op het evenwicht van het systeem en er uitdrukkelijk op heeft gewezen dat algoritmische profilering van burgers op basis van financiële gegevens indruist tegen de AVG en tegen artikel 8 van het Europees Verdrag voor de Rechten van de Mens. Het Nederlandse standpunt is volgens de spreker dan ook duidelijk: datamining of geautomatiseerde profilering wordt niet getolereerd.

Vervolgens verwijst de heer Van Quickenborne naar Zweden, dat de meest restrictieve aanpak hanteert door twee instanties te laten toezien op een systeem van

Le député explique également que la Cour constitutionnelle allemande a jugé ce système compatible avec le droit à l'autodétermination informationnelle, à condition qu'il reste strictement individuel et soumis à un contrôle indépendant. M. Van Quickenborne conclut dès lors que l'Allemagne n'a pas recours au *data mining* ni à la sélection automatisée des risques, puisque chaque demande requiert une décision humaine et une motivation. Le modèle allemand est ainsi considéré comme le système le plus respectueux des droits fondamentaux en Europe, tout en constituant une référence en matière d'efficacité.

L'intervenant poursuit avec l'exemple de l'Autriche, qui dispose d'un dispositif similaire au modèle allemand, mais avec une différence majeure: les données sont centralisées auprès de la Banque nationale autrichienne. En pratique, chaque banque doit transmettre quotidiennement les informations d'identification de ses clients à ce registre. La Banque nationale gère ce registre en tant qu'administrateur technique neutre et ne dispose d'aucun droit d'utiliser les données à des fins d'analyse. Par ailleurs, l'orateur souligne que la loi autrichienne interdit le *data mining*: les données ne peuvent être consultées que pour un objectif légalement défini et ne peuvent pas être traitées à des fins de profilage.

À propos des Pays-Bas, M. Van Quickenborne indique que le pays ne dispose pas d'un registre bancaire centralisé, mais fonctionne avec un réseau de systèmes d'information interconnectés. L'orateur précise que certaines instances, comme l'administration fiscale néerlandaise, disposent d'un accès électronique aux données bancaires dans le cadre de dossiers concrets. Les banques, quant à elles, sont légalement soumises à une obligation de déclaration. Il existe également un registre des bénéficiaires effectifs. L'orateur ajoute que la base juridique est répartie dans plusieurs textes légaux, lesquels prévoient que l'administration fiscale ne peut effectuer d'analyses générales de données sur les informations bancaires des citoyens. Des systèmes de sélection des risques existent bien au sein de l'administration, mais ils s'appliquent exclusivement aux données fiscales, et non aux données bancaires. Enfin, le député souligne que l'Autorité néerlandaise de protection des données veille à l'équilibre du système et a explicitement rappelé que le profilage algorithmique des citoyens sur la base de données financières est contraire au RGPD et à l'article 8 de la Convention européenne des droits de l'Homme. Selon lui, aux Pays-Bas, la position est donc claire: aucune tolérance pour le *data mining* ou le profilage automatisé.

M. Van Quickenborne poursuit avec l'exemple de la Suède et indique que ce pays adopte l'approche la plus restrictive, puisque deux instances supervisent un

specifieke verzoeken via een platform. De spreker legt uit dat wanneer een overheidsdienst, de politie of het gerecht wil nagaan of iemand een bankrekening heeft, ze een procedure moeten doorlopen die berust op een vraag-en-antwoordgebaseerde API: de banken antwoorden alleen met “ja” of “neen” op de vraag of de rekening bestaat. Op die manier worden geen gegevens bewaard of gecentraliseerd. Elk verzoek vereist bovendien een menselijke beslissing en wordt apart opgeslagen. De wetgeving op de verwerking van persoonsgegevens en de Zweedse grondwet schrijven voor dat elke verrichting evenredig moet zijn en beperkt moet blijven tot een welomlijnd doel. Geautomatiseerde profilering zonder menselijk ingrijpen is verboden. Een en ander toont volgens het lid aan dat Zweden het staatsgezag op het vlak van financiële controle wil beperken: het land kiest er bewust voor digitale infrastructuur alleen in te zetten voor individuele controles en niet voor grootscheepse analyses.

De spreker besluit zijn ronde van de Europese landen met Finland, dat sinds 2020 een centraal register van de bank- en betaalrekeningen bijhoudt, beheerd door de nationale financiële overheid. Dat register mag dan gecentraliseerd zijn, het is gebonden aan uitermate strikte regelgeving: de gegevens mogen alleen worden gebruikt door de politie, de douane, de belastingadministratie en de antiwitwascel. De heer Van Quickenborne verduidelijkt bovendien dat de Finse ombudsman voor gegevensbescherming onafhankelijk toezicht houdt en verwerkingen kan opschorten of sancties kan opleggen. Hoewel Finland opteert voor een gecentraliseerd systeem, eerbiedigt het land volgens de spreker zo toch de Europese beginselen van evenredigheid, doelmatigheid en subsidiariteit.

Afgaande op deze vijf voorbeelden stelt de heer Van Quickenborne vast dat zich een duidelijk Europees model aftekent en dat alle systemen zijn geënt op een formele, door een parlement aangenomen wet die de doelstellingen strikt afbakent. Bij al die systemen geldt bovendien een strikt verbod op datamining en geautomatiseerde profilering, gebeurt er toegangsregistratie, kennisgeving alsook wezenlijke controle en staan onafhankelijke autoriteiten met sanctiebevoegdheid in voor het toezicht. Volgens de spreker is aldus de Europese grondwettelijke gelijkgestemdheid gegroeid dat transparantie niet mag worden tot massasurveillance, een consensus die tot stand kwam dankzij de AVG en die berust op een evenredige en doelgerichte verwerking van gegevens, met menselijke tussenkomst.

Volgens de heer Van Quickenborne wijkt het plan dat België voor ogen heeft, totaal af van het Europese model. Hij herinnert eraan dat minister Jambon fiscale risicoprofielen in twee fases wil uitwerken: in een eerste fase

systeem fondé sur des requêtes spécifiques via une plateforme. L'orateur explique que lorsqu'un service public, la police ou la justice souhaite vérifier si une personne détient un compte bancaire, la procédure repose sur un mécanisme de question-réponse via une API: les banques répondent uniquement par “oui” ou “non” à la question de savoir si le compte existe. Ce faisant, aucune donnée n'est stockée ni centralisée. En outre, le membre précise que chaque requête nécessite une décision humaine et est enregistrée individuellement. La loi sur le traitement des données personnelles, ainsi que la Constitution suédoise, imposent que toute opération soit proportionnée et limitée à un objectif précis. Le profilage automatisé sans intervention humaine est interdit. Selon le député, la Suède illustre la volonté de limiter le pouvoir étatique en matière de contrôle financier: le pays choisit délibérément de ne pas utiliser l'infrastructure numérique pour des analyses massives, mais uniquement pour des vérifications individuelles.

Le député finit son tour d'horizon européen avec la Finlande qui dispose, depuis 2020, d'un registre centralisé des comptes bancaires et de paiement, géré par l'Autorité financière nationale. L'orateur précise que le dispositif, bien que centralisé, est encadré par une réglementation particulièrement stricte: les données ne peuvent être utilisées que par la police, la douane, l'administration fiscale et l'unité anti-blanchiment. En outre, M. Van Quickenborne précise que le médiateur pour la protection des données exerce un contrôle indépendant et peut suspendre des traitements ou imposer des sanctions. Ainsi, bien que la Finlande ait opté pour un système centralisé, l'orateur estime que le pays respecte pleinement les principes européens de proportionnalité, de finalité et de subsidiarité.

Fort de ces cinq exemples, M. Van Quickenborne constate qu'un modèle européen clair se dessine et que chacun de ces systèmes repose sur une loi formelle adoptée par un parlement, qui définit strictement les objectifs. En outre, le membre souligne que tous ces systèmes interdisent explicitement le *data mining* et le profilage automatisé, prévoient la journalisation des accès, la notification et un contrôle effectif, et confient la surveillance à des autorités indépendantes dotées de pouvoirs de sanction. Selon l'orateur, il existe ainsi une convergence constitutionnelle européenne: la transparence ne doit pas se transformer en surveillance de masse, et le RGPD a conduit à ce consensus fondé sur une gestion proportionnée et ciblée des données, avec intervention humaine.

À propos de la Belgique, M. Van Quickenborne estime que le plan envisagé s'écarte totalement de ce modèle européen. Il rappelle que l'objectif du ministre Jambon est de développer des profils de risque fiscaux selon

zal het risicoprofiel an sich worden vastgesteld, waarna dat profiel in een tweede fase op individuele dossiers zal worden toegepast. Volgens de heer Van Quickenborne gaat het duidelijk om een vorm van datamining, die in bovenvermelde Europese landen expliciet verboden is. Hij onderstreept dat België door die keuze verder dreigt af te wijken van de Europese richtlijnen, die elke verwerking van gevoelige gegevens strikt afhankelijk maken van evenredigheid en subsidiariteit. Volgens hem is het fundamentele verschil met de vijf onderzochte landen niet alleen van technische, maar ook van juridische aard: in die landen is de verwerking van financiële gegevens op het subsidiariteitsbeginsel gestoeld, wat betekent dat de desbetreffende informatie alleen wordt opgevraagd als de burger niet meewerkt of als er concrete aanwijzingen van onregelmatigheden zijn. Het komt hem voor dat de regering die logica wil omdraaien door actief een profiel op te maken van alle burgers en pas in een volgende fase te kiezen wie wordt gecontroleerd. Hij is gewonnen voor de werkwijze in de vijf bovengenoemde landen, waarbij van het beginsel van het menselijke toezicht wordt uitgegaan. Met het plan van minister Jambon zou die menselijke tussenkomst volgens hem minimaal zijn en zou er *a posteriori* niet de minste transparantie zijn, zodat burgers naar alle waarschijnlijkheid niet te weten zullen komen of en wanneer hun bankgegevens zijn gebruikt.

Volgens de heer Van Quickenborne hollen die structurele verschillen het recht op eerlijk en transparant bestuur uit, aangezien met een systeem dat burgers preventief aan een algoritmische filtering onderwerpt, men de fiscale controle als uitgangspunt loslaat ten voordele van een evolutie naar surveillancetechnologie. Volgens hem bestaat de lijn die op Europees niveau wordt aangehouden en die wordt bevestigd in de analyseresultaten van de vijf onderzochte landen, erin dat toegang tot financiële gegevens enkel binnen de grenzen van de evenredigheid mogelijk is.

Het *money control*-project waarvan minister Jambon de trekker is, overschrijdt volgens het lid die grenzen, aangezien het niet langer vanuit een individuele en evenredige basis vertrekt, maar een systematische en preventieve aanpak hanteert. De heer Van Quickenborne benadrukt dat de vijf onderzochte systemen nochtans aantonen dat fiscale doelmatigheid perfect bestaanbaar is met de bescherming van de grondrechten, op voorwaarde dat drie structurele waarborgen worden nageleefd: decentralisatie dan wel gecontroleerde centralisatie, wettigheid en menselijk toezicht, alsook transparantie. Volgens de heer Van Quickenborne tonen de voorbeelden van de vijf landen aan dat transparantie, doelmatigheid en de bescherming van de persoonlijke levenssfeer elkaar niet uitsluiten, op voorwaarde dat de Staat zichzelf grenzen

deux étapes: dans un premier temps, établir un profil de risque; dans un second temps, appliquer ce profil à des dossiers individuels. Selon l'orateur, il s'agit clairement d'une forme de *data mining*, explicitement interdite dans les pays européens susmentionnés. Le député souligne que ce choix risque d'éloigner la Belgique des directives européennes, qui imposent que la proportionnalité et la subsidiarité soient des conditions indispensables pour tout traitement de données sensibles. Selon lui, la différence fondamentale avec les cinq pays étudiés n'est pas seulement technique, mais aussi juridique: dans ces États, le traitement des données financières repose sur le principe de subsidiarité, c'est-à-dire que les informations ne sont demandées qu'en cas de non-coopération du citoyen ou lorsqu'il existe des indices concrets d'irrégularité. L'orateur estime que le gouvernement semble vouloir inverser cette logique en profilant activement l'ensemble des citoyens avant de sélectionner ceux qui seront contrôlés. Le député salue l'exemple des cinq pays susmentionnés qui respectent le principe de supervision humaine. Avec le plan du ministre Jambon, il estime que cette intervention serait minimale, sans la moindre transparence *a posteriori*, de sorte que les citoyens risquent d'ignorer si, et à quel moment, leurs données bancaires ont été utilisées.

M. Van Quickenborne estime que ces différences structurelles touchent au cœur du droit à une administration équitable et transparente puisqu'un système qui soumet préventivement les citoyens à un filtrage algorithmique abandonne la logique du contrôle fiscal et évolue vers une technologie de surveillance. Selon lui, la ligne européenne, confirmée par l'analyse des cinq pays analysés, reconnaît que l'accès aux données financières ne peut exister qu'à l'intérieur des limites de la proportionnalité.

Or, selon le député, le projet *money control* porté par le ministre Jambon franchit ces limites, car il ne fonctionne plus de manière individuelle et proportionnée, mais systématique et préventive. L'orateur souligne pourtant que les cinq systèmes étudiés démontrent que l'efficacité fiscale est parfaitement compatible avec la protection des droits fondamentaux, à condition de respecter trois garanties structurelles: Une décentralisation ou une centralisation contrôlée, la légalité et la supervision humaine, et la transparence. Le député estime que les exemples des cinq pays prouvent que transparence, efficacité et protection de la vie privée ne sont pas incompatibles, à condition que l'État s'impose des limites. Selon lui, la Belgique, en revanche, semble s'engager sur une voie qui mine les fondements de cette

oplegt. Volgens hem lijkt België echter een weg in te slaan die de fundamenteën van die Europese rechtscultuur ondermijnt en evolueert de aanpak van ons land van gerichte controle naar preventieve surveillance.

De spreker gaat vervolgens in op het Duitse model, te beginnen met het centrale rechtsinstrument dat de Duitse autoriteiten, en met name de belastingdienst, toegang geeft tot de basisinformatie betreffende de in Duitsland aangehouden bankrekeningen en effectenrekeningen. De heer Van Quickenborne licht toe dat dit instrument werd ingevoerd in een context van toenemende internationale druk om witwassen, fiscale fraude en terrorismefinanciering tegen te gaan.

Volgens de spreker berust dat model niet op een centrale databank waarin alle informatie over de rekeningen wordt opgeslagen, want de informatie wordt alleen opgevraagd bij een concreet vermoeden of in geval van onderzoeksbehoeften. Hij wijst er ook op dat de Duitse belastingdienst tot het begin van de jaren 2000 over geen enkel systematisch instrument beschikte om de bankrekeningen van de belastingplichtigen te achterhalen. Ze kon alleen informatie verkrijgen via de rechtbanken of in het raam van specifieke strafrechtelijke onderzoeken. Na de aanslagen van 11 september 2001 heeft de Duitse federale regering meerdere wetten tegen witwassen en terrorismefinanciering aangenomen teneinde meer fiscale doeltreffendheid tot stand te brengen via een snellere toegang tot bankgegevens. Tevens werd beoogd de strijd tegen dergelijke praktijken op te voeren via een betrouwbaar gegevensuitwisselingsmechanisme.

De spreker benadrukt dat de Duitse wetgever echter heeft aangedrongen op het noodzakelijke en evenredige karakter van elke raadpleging: de financiële instellingen moeten weten welke autoriteiten toegang hebben tot hun gegevens, en de wet schrijft voor dat bepaalde basisgegevens, met name de identiteit van de rekeninghouder, tien jaar moeten worden bewaard. Wat dat betreft, licht de spreker toe dat de Duitse federale autoriteit voor financieel toezicht fungeert als toegangspunt en controleorgaan: zij ontvangt de aanvragen van de bevoegde autoriteiten en stuurt die automatisch door naar de betrokken banken, zonder de gegevens te kunnen raadplegen of gebruiken. Elke aanvraag wordt geregistreerd en vijf jaar bewaard, zodat achteraf een controle door de gegevensbeschermingsautoriteit of door het gerecht kan plaatsvinden. De gegevens mogen alleen worden gebruikt in het raam van belastingen, strafrechtelijke onderzoeken, sociale controles, de invordering van schulden ten aanzien van de overheid en financieel toezicht.

De heer Van Quickenborne wijst er bovendien op dat de Duitse wetgeving de belastingdienst de mogelijkheid

culture juridique européenne: le passage d'un contrôle ciblé à une surveillance préventive.

Le député souhaite ensuite s'attarder sur le modèle allemand, à commencer par l'instrument juridique central permettant aux autorités allemandes, et en particulier à l'administration fiscale, d'accéder aux informations de base relatives aux comptes bancaires et aux comptes-titres détenus en Allemagne. M. Van Quickenborne explique que cet outil a été instauré dans un contexte de pression internationale croissante visant à lutter contre le blanchiment d'argent, la fraude fiscale et le financement du terrorisme.

Selon l'orateur, ce modèle ne repose pas sur une base de données centrale où seraient stockées toutes les informations sur les comptes; celles-ci ne sont demandées qu'en cas de soupçon concret ou de besoin d'enquête. Il rappelle également que, jusqu'au début des années 2000, l'administration fiscale allemande ne disposait d'aucun instrument systématique pour identifier les comptes bancaires des contribuables. Elle ne pouvait obtenir des informations qu'au travers des tribunaux ou dans le cadre d'enquêtes pénales spécifiques. À la suite des attentats du 11 septembre 2001, le gouvernement fédéral allemand a adopté une série de lois contre le blanchiment et le financement du terrorisme, afin d'accroître l'efficacité fiscale en permettant un accès plus rapide aux informations bancaires et de renforcer la lutte contre ces pratiques par un mécanisme fiable d'échange de données.

Le député souligne que le législateur allemand a toutefois insisté sur le caractère nécessaire et proportionné de chaque consultation: les établissements financiers doivent savoir quelles autorités peuvent accéder à leurs données, et la loi impose de conserver pendant dix ans certaines données de base, notamment l'identité du titulaire. Dans ce cadre, le membre explique que l'autorité fédérale allemande de supervision financière agit comme point d'accès et de contrôle: elle reçoit les demandes des autorités compétentes et les transmet automatiquement aux banques concernées, sans pouvoir consulter ni utiliser les données. Chaque demande est enregistrée et conservée cinq ans pour permettre un contrôle *a posteriori* par l'autorité de protection des données ou par la justice. Les données ne peuvent être utilisées que pour la fiscalité, les enquêtes pénales, les contrôles sociaux, le recouvrement de créances publiques et la supervision financière.

M. Van Quickenborne indique également que la législation allemande permet à son administration fiscale

biedt een verzoek in te dienen via de Duitse federale overheid voor financieel toezicht. Wanneer er fiscaal relevante feiten aanwezig zijn, kan de belastingdienst dus een raadpleging starten om de nodige gegevens te verzamelen voor het vaststellen van de belasting, voor zover dat echt nodig is en het geen onevenredige inbreuk op de privacy vormt. De spreker licht toe dat die raadplegingsprocedure in Duitsland in drie fasen verloopt. Om te beginnen motiveert de bevoegde belastingdienst schriftelijk waarom de raadpleging nodig is. Het verzoek wordt vervolgens elektronisch verzonden naar de Duitse federale financiële toezichthouder, die contact opneemt met de betrokken bank(en) en het resultaat terugstuurt naar de verzoekende overheid. De spreker wijst erop dat de Duitse wetgeving vereist dat de belastingdienst de betrokkene na de raadpleging op de hoogte brengt, tenzij een dergelijke kennisgeving het doel van het onderzoek in gevaar zou brengen. Die verplichting vloeit voort uit de principes van de AVG en de Duitse federale wet op de gegevensbescherming. De heer Van Quickenborne benadrukt dat Duitsland bewust heeft gekozen voor een gedecentraliseerd systeem, een aanpak die wordt ingegeven door de eerbiediging van het fundamentele recht op informatiele zelfbeschikking en door de Duitse traditie van federale bestuurlijke autonomie.

De spreker gaat voorts in op de rol van de kredietinstellingen, die wettelijk verplicht zijn de basisgegevens van de rekeningen op te slaan in een databank die voldoet aan het standaardformaat dat wordt voorgeschreven door de Duitse federale financiële toezichthouder. Die gegevens moeten onmiddellijk worden geactualiseerd in geval van wijziging en tot tien jaar na het afsluiten van de rekening worden bewaard, wat overeenkomt met de praktijk in België. Hoewel ze onder toezicht staan van de Duitse federale financiële toezichthouder, worden de banken beschouwd als verwerkingsverantwoordelijken in de zin van de Duitse federale wet op de gegevensbescherming. Elke instelling moet dus een functionaris voor gegevensbescherming aanstellen.

Daarnaast benadrukt de heer Van Quickenborne dat de Duitse belastingdienst wettelijk alleen een raadpleging mag starten wanneer dat concreet fiscaal belang heeft, bijvoorbeeld wanneer men verborgen inkomsten of activa moet nagaan, of wanneer minder ingrijpende middelen niet volstaan. Bovendien vereist raadpleging toestemming van een hiërarchische meerdere. De inspecteur stelt een met redenen omkleed schriftelijk verzoek op en stuurt het vervolgens elektronisch door. Het antwoord bevat louter een lijst van de betrokken rekeningen en gevolmachtigden, zonder informatie over de transacties. Indien aanvullende gegevens nodig zijn, kunnen die slechts worden verkregen via een afzonderlijke procedure, met toestemming van de belastingplichtige of op grond van een rechterlijke beslissing. De spreker licht toe dat

d'effectuer une demande via l'autorité fédérale allemande de supervision financière. Ainsi, l'autorité fiscale peut initier une consultation lorsqu'il existe des faits fiscalement pertinents, afin d'établir des éléments nécessaires à la détermination de l'impôt, pour autant que cela soit indispensable et ne constitue pas une atteinte disproportionnée à la vie privée. L'orateur explique que cette procédure de consultation en Allemagne se déroule en trois étapes: le service fiscal compétent motive par écrit la nécessité de la consultation. La demande est ensuite transmise électroniquement à l'autorité fédérale allemande de supervision financière, qui sollicite alors la ou les banques concernées et renvoie le résultat à l'autorité requérante. L'orateur précise que la législation allemande impose à l'administration fiscale d'informer la personne concernée après la consultation, sauf si cette notification compromettrait l'objectif de l'enquête. Cette obligation découle des principes du RGPD et de la loi fédérale allemande sur la protection des données. M. Van Quickenborne met en exergue le fait que l'Allemagne a délibérément opté pour un système décentralisé, une approche qui est justifiée par le respect du droit fondamental à l'autodétermination informationnelle et par la tradition allemande d'autonomie administrative fédérale.

L'orateur aborde ensuite le rôle des établissements de crédit, qui sont légalement tenus de conserver les données de base des comptes dans une base de données conforme au format standard prescrit par l'autorité fédérale allemande de supervision financière. Ces données doivent être mises à jour immédiatement en cas de modification et conservées pendant dix ans après la clôture du compte, ce qui correspond à la pratique belge. Bien que placées sous la supervision de l'autorité fédérale allemande de supervision financière, les banques sont considérées comme responsables du traitement au sens de la loi fédérale allemande sur la protection des données, et chaque établissement doit désigner un délégué à la protection des données.

En outre, M. Van Quickenborne souligne que l'administration fiscale allemande ne peut légalement initier une consultation que lorsqu'il existe un intérêt fiscal concret, par exemple pour vérifier des revenus ou des avoirs dissimulés, lorsque des moyens moins intrusifs ne suffisent pas, et avec l'approbation d'un supérieur hiérarchique. L'inspecteur motive la demande par écrit, qui est ensuite transmise électroniquement. La réponse contient uniquement une liste des comptes et des mandataires concernés, sans informations sur les transactions. Si des détails supplémentaires sont nécessaires, ils ne peuvent être obtenus que par une procédure distincte, avec le consentement du contribuable ou sur décision judiciaire. L'orateur précise que d'autres autorités peuvent également introduire une demande, notamment les

ook andere autoriteiten een verzoek kunnen indienen, onder meer de gerechtelijke autoriteiten in het kader van strafonderzoeken. Elke overheid heeft haar eigen wettelijke basis en strikte voorwaarden; er bestaat dus geen algemene toegang. De Duitse federale financiële toezichthouder controleert daarom systematisch de bevoegdheid en de wettelijke basis van elk verzoek.

De spreker voegt eraan toe dat bij elke raadpleging een logbestand wordt gecreëerd met de datum en de tijd van het verzoek, de identiteit van de verzoekende instantie, de ingeroepen rechtsgrondslag, het resultaat (positief of negatief) en de identificatie van de geraadpleegde bank. Die bestanden moeten minstens vijf jaar worden bijgehouden, tegenover zes maanden in België, en kunnen worden ingezien door de federale gegevensbeschermingsautoriteit of door de parlementaire toezichthoudende dienst.

De heer Van Quickenborne heeft het vervolgens over de toegangsvoorwaarden in Duitsland en over de Duitse raadplegingsprocedure, die volledig geautomatiseerd verloopt, via een elektronisch belastingaangifteplatform. De spreker legt uit dat de bevoegde instantie het verzoek digitaal indient met behulp van een gestandaardiseerd formulier, waarin de rechtsgrondslag wordt vermeld, alsook de identificatie van de betrokkene, de concrete reden voor de raadpleging en de bevestiging dat de maatregel evenredig is. De Duitse federale financiële toezichthouder verifieert de authenticiteit van het verzoek en stuurt die door naar alle betrokken kredietinstellingen. Elke bank reageert automatisch binnen enkele seconden en geeft bij een positief resultaat de vereiste basisgegevens door. De Duitse federale financiële toezichthouder consolideert vervolgens de antwoorden en stuurt ze terug naar de verzoekende instantie. Na afsluiting van de procedure ontvangt de belastingplichtige een melding van de raadpleging, behalve indien een strafonderzoek loopt of indien de melding het doel van het onderzoek in gevaar zou brengen. De betrokkene heeft dan het recht op toegang tot de geregistreerde gegevens en kan een klacht indienen.

Het lid grijpt de verwijzing naar die procedure aan om te herinneren aan het grondbeginsel achter de informatieve zelfbeschikking, alsook aan het door het Duitse grondwettelijk hof toegepaste evenredigheidstoezicht, dat berust op vier criteria: een rechtmatig doel (zoals de strijd tegen belastingfraude en witwaspraktijken), de geschiktheid (de raadplegingsprocedure is geschikt om verborgen rekeningen op te sporen), de noodzaak en de evenredigheid, in de strikte betekenis.

De spreker vestigt ook de aandacht op de relatie met artikel 8 van het Europees Verdrag van de Rechten van de Mens en met de AVG, aangezien beide instrumenten

autorités judiciaires dans le cadre d'enquêtes pénales. Chaque autorité dispose de sa propre base légale et de conditions strictes: il n'existe pas d'accès générique, de sorte que l'autorité fédérale allemande de supervision financière vérifie systématiquement la compétence et la base légale de chaque demande.

L'intervenant ajoute que chaque consultation génère un fichier journal contenant la date et l'heure de la demande, l'identité de l'autorité requérante, la base légale invoquée, le résultat (positif ou négatif) et l'identification de la banque consultée. Ces fichiers doivent être conservés pendant au moins cinq ans, contre six mois en Belgique, et peuvent être contrôlés par l'autorité fédérale de protection des données ou par le service parlementaire de contrôle.

M. Van Quickenborne en vient ensuite à la procédure de consultation et aux conditions d'accès en Allemagne, qui est intégralement automatisée via une plateforme électronique de déclaration fiscale. L'orateur explique que l'autorité compétente introduit la demande de manière numérique au moyen d'un formulaire standardisé, mentionnant la base légale, l'identification de la personne concernée, la raison concrète de la consultation et la confirmation que la mesure est proportionnée. L'autorité fédérale allemande de supervision financière vérifie l'authenticité de la demande et la transmet à toutes les institutions de crédit concernées. Chaque banque répond automatiquement en quelques secondes et, en cas de résultat positif, communique les données de base requises. L'autorité fédérale allemande de supervision financière consolide ensuite les réponses et les renvoie à l'autorité requérante. Après la clôture de la procédure, le contribuable reçoit une notification de la consultation, sauf si une enquête pénale est en cours ou si la notification compromettrait l'objectif de l'investigation. La personne concernée dispose alors d'un droit d'accès aux données enregistrées et peut introduire une plainte.

L'évocation de cette procédure permet au député de rappeler le principe fondamental de l'autodétermination informationnelle, ainsi que le contrôle de proportionnalité appliqué par la Cour constitutionnelle fédérale allemande qui repose sur quatre critères: un objectif légitime (comme la lutte contre la fraude fiscale et le blanchiment d'argent), l'adéquation (la procédure de consultation est appropriée pour identifier des comptes dissimulés), la nécessité et la proportionnalité au sens strict.

L'orateur rappelle également la relation avec l'article 8 de la Convention européenne des droits de l'homme et avec le RGPD, puisque ces deux instruments encadrent

een kader vormen voor de Duitse regeling. Hij verduidelijkt dat de Europese rechtspraak erkent dat belastingcontrole kan neerkomen op een inmenging in de persoonlijke levenssfeer, maar gerechtvaardigd is wanneer ze bij wet werd geoorloofd en noodzakelijk is in een democratische samenleving. Bovendien vereist de AVG dat elke verwerking een duidelijke wettelijke basis heeft en vergezeld gaat van garanties inzake transparantie, doelbinding en evenredigheid. In dat verband benadrukt de heer Van Quickenborne dat Duitsland niet aan automatische profilering doet, noch aan het massale kruisen van gegevens, alsook dat de burgers er *a posteriori* recht hebben op informatie evenals op beroepsmogelijkheden. Om die redenen wijst hij erop dat het Duitse model vaak wordt beschouwd als een goede praktijk binnen de Europese Unie, omdat het belastingefficiëntie combineert met grondwettelijke garanties.

De heer Van Quickenborne verwijst naar de Duitse wetgeving en rechtspraak en wijst erop dat de aldaar bestaande verplichting tot het bijhouden van gegevens drie hoofddoelstellingen nastreeft: controleerbaarheid, door de autoriteiten in staat te stellen *a posteriori* de wettelijkheid van de raadplegingen te controleren; traceerbaarheid, waarbij de burgers een toegangsrecht krijgen om te weten welke overheden hun gegevens hebben geraadpleegd; en tot slot preventie, door misbruik te ontmoedigen dankzij het vooruitzicht op een latere controle. In dat verband wijst de spreker er nogmaals op dat in Duitsland die logbestanden gedurende vijf jaar worden bewaard, terwijl dat in België slechts zes maanden is, wat een aanzienlijk verschil uitmaakt op het stuk van transparantie en bescherming van rechten.

De heer Van Quickenborne benadrukt dat het bijhouden van een logboek ook een preventieve functie heeft: ambtenaren weten dat elke raadpleging wordt geregistreerd, wat misbruik afschrikt. Hij vergelijkt dat mechanisme met dat van het Rijksregister van de natuurlijke personen in België, waar elke raadpleging door een politieagent wordt getraceerd en kan leiden tot sancties in geval van misbruik. De logbestanden hebben bovendien een bewijskrachtige functie: bij een rechtsgeschil kunnen ze als bewijs dienen.

De spreker wijst er ook op dat de Duitse wetgeving vereist dat de logbestanden worden gegenereerd via een onveranderlijk auditspoor en dat elke wijziging van een logbestand elektronisch wordt ondertekend. Dat auditspoor wordt jaarlijks geverifieerd door onafhankelijke auditors, terwijl het Duitse federale rekenhof periodieke audits op het systeem uitvoert, die betrekking hebben op de gegevensintegriteit, het toegangsbeheer en de naleving van de archiveringstermijnen. Elke bank moet ook een complianceofficer aanduiden die verantwoordelijk is voor de uitvoering van steekproefcontroles op de

le système allemand. Il précise que la jurisprudence européenne reconnaît que les contrôles fiscaux peuvent constituer une ingérence dans la vie privée, mais que celle-ci est justifiée lorsqu'elle est prévue par la loi et nécessaire dans une société démocratique. De plus, le RGPD impose que tout traitement repose sur une base légale claire et s'accompagne de garanties de transparence, de limitation des finalités et de proportionnalité. À cet égard, M. Van Quickenborne souligne que l'Allemagne n'a pas recours au profilage automatique ni au croisement massif de données et que les citoyens disposent d'un droit à l'information *a posteriori* ainsi que de voies de recours. Pour ces raisons, le député indique que le modèle allemand est souvent considéré comme une bonne pratique au sein de l'Union européenne, car il combine efficacité fiscale et garanties constitutionnelles.

En citant la législation et la jurisprudence allemandes, M. Van Quickenborne rappelle l'obligation de journalisation en Allemagne, qui poursuit trois objectifs principaux: la contrôlabilité, permettant aux autorités de vérifier *a posteriori* la légalité des consultations; la traçabilité, offrant aux citoyens un droit d'accès pour savoir quelles autorités ont consulté leurs données; et enfin la prévention, en dissuadant les abus grâce à la perspective d'un contrôle ultérieur. À ce propos, l'orateur souligne à nouveau qu'en Allemagne, ces journaux sont conservés pendant cinq ans, contre seulement six mois en Belgique, ce qui constitue une différence notable en matière de transparence et de protection des droits.

M. Van Quickenborne insiste sur le fait que la journalisation joue également un rôle préventif: les fonctionnaires savent que chaque consultation est enregistrée, ce qui dissuade les abus. Il compare ce mécanisme à celui du registre national en Belgique, où toute consultation par un policier est tracée et peut entraîner une sanction en cas d'abus. Les journaux remplissent en outre une fonction probatoire: en cas de litige judiciaire, ils peuvent servir de preuve.

L'intervenant précise également que la législation allemande impose que les journaux soient générés via une piste d'audit inaltérable et que toute modification d'un fichier journal soit signée électroniquement. Cette piste d'audit est vérifiée chaque année par des auditeurs indépendants, tandis que la Cour des comptes fédérale allemande réalise des audits périodiques du système, portant sur l'intégrité des données, la gestion des accès et le respect des délais d'archivage. Chaque banque doit, de son côté, désigner un responsable conformité chargé d'effectuer des contrôles par sondage sur les

raadplegingen en die moet rapporteren aan de directie en de externe auditor.

Het lid wijst erop dat de onafhankelijke toezichthoudende autoriteit in Duitsland uitgebreide bevoegdheden heeft: ze kan onaangekondigde inspecties uitvoeren, de openbaarmaking van logboeken en technische documentatie eisen, aanbevelingen of injuncties uitvaardigen in geval van een schending van de AVG en klachten van burgers behandelen. Ze brengt elk jaar een verslag uit aan de Bondsdag en de federale regering. De belangrijkste controlepunten hebben betrekking op het doel van de raadplegingen, de proportionaliteit van de aanvragen, de veiligheid van de systemen en de naleving van de verplichting om de burgers te informeren.

Tot slot gaat de spreker in op de coördinatie tussen de Duitse federale gegevensbeschermingsautoriteit en de gegevensbeschermingsautoriteiten van de deelstaten, die een uniforme toepassing van het evenredigheidsbeginsel in het hele land garandeert. In geval van inbreuken kan de federale autoriteit een formeel advies uitbrengen, de tijdelijke schorsing van de verwerking bevelen of de zaak aanhangig maken bij de federale administratieve rechtbank teneinde een sanctie te doen opleggen. Op basis van statistieken die zijn gepubliceerd door het Duitse federale ministerie van Financiën, wijst de heer Van Quickenborne erop dat het merendeel van de verzoeken wordt ingegeven door fiscale motieven, voornamelijk het controleren van niet-aangegeven vermogens of verdachte inkomstenstromen. De overige verzoeken zijn afkomstig van gerechtelijke autoriteiten en socialezekerheidsinstanties, wat een doeltreffende procedure garandeert die voldoet aan de gegevensbeschermingsvereisten en die de beginselen van de rechtsstaat respecteert.

De *Bundestag* heeft het systeem ook herhaaldelijk geëvalueerd, wat dus in België niet gebeurt: het CAP wordt niet geëvalueerd.

Nochtans, artikel 333 in haar laatste lid zegt dat de minister jaarlijks een verslag moet overmaken aan het Parlement, en dat zij dat dan bezorgen aan de commissie voor Financiën & Begroting. Het lid heeft van het secretariaat van de commissie geen verslagen mogen ontvangen: hij veronderstelt dat er dus geen verslagen zijn. Terwijl de wet expliciet voorziet dat er een verslag moet opgemaakt worden elk jaar sinds de inwerking van de wet van 2008, dus vanaf 2012.

In Duitsland daarentegen heeft de *Bundestag* het systeem herhaaldelijk geëvalueerd via rapporten van de commissie voor Financiën. Er zijn blijkbaar verslagen gemaakt in Duitsland in 2012, 2017 en 2021. Er blijkt dat:

consultations et de rendre compte à la direction ainsi qu'à l'auditeur externe.

Le député précise que l'autorité indépendante de contrôle en Allemagne dispose de compétences étendues: elle peut effectuer des inspections inopinées, exiger la communication des journaux et de la documentation technique, formuler des recommandations ou des injonctions en cas de violation du RGPD et traiter les plaintes des citoyens. Elle publie chaque année un rapport adressé au Bundestag et au gouvernement fédéral. Les principaux points de contrôle portent sur la finalité des consultations, la proportionnalité des demandes, la sécurité des systèmes et le respect de l'obligation d'information des citoyens.

Enfin, l'orateur évoque la coordination entre l'instance fédérale allemande de protection des données et les autorités de protection des données des Länder, qui garantit une application uniforme du principe de proportionnalité sur l'ensemble du territoire. En cas de manquement, l'instance fédérale peut émettre un avis formel, ordonner la suspension temporaire du traitement ou saisir le tribunal administratif fédéral afin d'obtenir une sanction. Sur la base de statistiques publiées par le ministère fédéral allemand des Finances, M. Van Quickenborne souligne que la majorité des demandes sont motivées par des objectifs fiscaux, principalement la vérification de patrimoines non déclarés ou de flux de revenus suspects, les autres provenant des autorités judiciaires et des organismes de sécurité sociale, ce qui garantit une procédure efficace, conforme aux exigences de protection des données et respectueuse des principes de l'État de droit.

Le *Bundestag* a également évalué le système à plusieurs reprises, ce qui n'est donc pas le cas en Belgique, où le PCC n'est pas évalué.

L'article 333, dernier alinéa, prévoit pourtant que le ministre doit transmettre chaque année un rapport au Parlement, qui doit ensuite le communiquer à la commission des Finances et du Budget. Or, le membre n'a pas reçu de rapports de la part du secrétariat de la commission: il suppose donc que ces rapports n'existent pas, et ce, alors que la loi prévoit explicitement qu'un rapport doit être établi chaque année depuis l'entrée en vigueur de la loi de 2008, c'est-à-dire à partir de 2012.

En Allemagne, en revanche, le *Bundestag* a évalué le système à plusieurs reprises dans des rapports établis par la commission des Finances. Des rapports y ont manifestement été établis en 2012, 2017 et 2021. Il en ressort que:

1. Het is mogelijk om in een vroeg stadium verborgen rekening te detecteren en fraude sneller aan te pakken. Dus hoge efficiëntie in Duitsland.

2. Weinig klachten: het aantal geregistreerde klachten blijft zeer laag (minder dan 0,05 %). De administratieve lasten voor banken zijn beheersbaar (5 euro per aanvraag).

De *Bundestag* heeft gezegd dat de constitutionele robuustheid verzekerd is. Er is geen aanwijzing dat de procedure de privacy of mensenrechten schendt zolang zij binnen de wettelijke grenzen worden toegepast.

Er zijn toch twee verbeterpunten vermeld:

1. De kennisgevingsplicht aan burgers wordt te vaak uitgesteld of achterwege gelaten vooral bij langdurige fiscale onderzoeken.

2. De technische afhankelijkheid zou op termijn tot capaciteitsproblemen kunnen leiden. Men onderzoekt daarom alternatieve *cloud*-architectuur.

In de literatuur wordt het Duitse model vaak geciteerd.

Toch bestaan er nuances. Er zijn rechtswetenschappers die hierop wijzen dat de *ex-post* toetsing via logging en audits weliswaar grondrechtelijk voldoende is maar in de praktijk sterk afhangt van de midden van de toezichthouders. Er zijn ook privacy-NGO's in Duitsland zoals *Digital Courage* en *Netzpolitik.org* die bedenkingen hebben: zij bepleiten voor een versterkt transparantieregister zodat burgers proactief kunnen nagaan of hun gegevens zijn heruitgelegd. Dat kan misschien aanleiding geven tot een amendement.

De bankfederaties benadrukken dat de bewaarplicht van tien jaar te lang is, gelet op de kost van archivering. Er is toch wel wat druk in Duitsland om die termijn wat te verminderen.

Er bestaat een brede consensus dat het reglement inzake de raadpleging van gegevens in zijn huidige vorm grondrechtelijk aanvaardbaar en technisch veilig is, maar dat voortdurende evaluatie nodig blijft om wat men noemt *function creep* (dat dat iedere keer groter en groter wordt) te voorkomen. In Duitsland is de *Bundestag* daarover geraadplecht geweest. En er is weliswaar ook die fameuze uitspraak van 12 juli 2007, waarin het Federaal Constitutioneel Hof het systeem grondwettig verklaarde mits individuele proportionaliteit en transparantie wordt

1. Le système allemand permet de détecter les comptes cachés à un stade précoce et de lutter plus rapidement contre la fraude. Ce système est donc très efficace.

2. Les dépôts de plainte sont rares: le nombre de plaintes enregistrées reste très faible (moins de 0,05 %). Les charges administratives qui incombent aux banques sont maîtrisables (5 euros par demande).

Le *Bundestag* a indiqué que la robustesse constitutionnelle du dispositif était assurée. Rien n'indique que la procédure porte atteinte à la vie privée ou aux droits de l'homme tant qu'elle est appliquée dans le respect des limites fixées par la loi.

Deux points d'amélioration ont toutefois été mentionnés:

1. L'obligation de notification aux citoyens est trop souvent reportée ou omise, surtout dans le cadre d'enquêtes fiscales de longue durée.

2. La dépendance technique pourrait, à terme, entraîner des problèmes de capacité. C'est pourquoi les autorités allemandes examinent une architecture alternative reposant sur le recours à une solution nuagique (*cloud*).

Le modèle allemand est souvent cité dans la littérature.

Mais les avis sont parfois nuancés. Certains juristes soulignent que s'il est vrai que le contrôle *a posteriori* au travers de la journalisation et des audits est suffisant selon la Constitution, il dépend néanmoins fortement, en pratique, des moyens dont disposent les autorités de contrôle. Certaines ONG allemandes spécialisées dans la protection de la vie privée, telles que *Digital Courage* et *Netzpolitik.org*, émettent également certaines réserves: elles préconisent un renforcement du registre de transparence pour que les citoyens puissent vérifier de manière proactive si leurs données ont été réutilisées. Cela pourrait peut-être donner lieu à un amendement.

Les fédérations bancaires soulignent que la durée de l'obligation de conservation de dix ans est excessive, compte tenu du coût de l'archivage. Certaines voix se font entendre en Allemagne pour réduire cette durée.

Il existe un large consensus sur le fait que le règlement relatif à la consultation des données est en l'état constitutionnellement acceptable et techniquement sûr, mais qu'une évaluation continue reste nécessaire afin d'éviter ce que l'on appelle le *function creep* (c'est-à-dire une extension progressive et incontrôlée). En Allemagne, le *Bundestag* a été consulté à ce sujet. Le Tribunal constitutionnel fédéral a par ailleurs considéré, dans sa célèbre décision du 12 juillet 2007, que le système était conforme à la Constitution pour autant

gewaarborgd. Er zijn nog latere uitspraken geweest van verschillende rechtbanken in Duitsland, die die uitspraken hebben verfijnd. Die rechtspraak toont een constante lijn: het Rekenhof toestaat gegevensuitwisseling, maar enkel binnen een strikt doel- en proportionaliteitskader.

In 2022 waren er maar liefst dertig audits uitgevoerd. In vier gevallen werden kleine procedurele tekortkomingen vastgesteld. Het ging om onvolledige logging of vertraagde kennisgeving. Maar geen enkel geval leidde tot een formele sanctie.

Er is natuurlijk de methodologische uitgangspunten. De beoordeling vergt een dubbele invalshoek. Enerzijds moet worden onderzocht in welke mate het systeem zijn beoogde doel, de bestrijding van belastingen ontduiken, witwassen, en of het een onrechtmatige uitkering effectief bereikt. En anderzijds is ook noodzakelijk te evalueren of deze resultaten worden behaald met inachtneming van de grondrechten. Het is die voortdurende balans tussen fraudebestrijding en de grondrechten die moet worden bewaakt: de eisen van proportionaliteit, subsidiariteit en doelwinning.

In de Duitse doctrine wordt deze dubbele invalshoek vaak omschreven als het evenwicht tussen belastingefficiëntie en bescherming van grondrechten. Het federaal constitutioneel hof (Bundesverfassungsgericht, B-VG) benadrukt herhaaldelijk dat beide dimensies niet in tegenstelling hoeven te staan met elkaar, maar mits de nodige wettelijke kaders duidelijk voorspelbaar en controleerbaar zijn.

De analyse die wordt gemaakt, berust op de teksten van artikel 24c van de *Kreditwesengesetz* (KWG), artikel 93 van de *Abgabenordnung* (AO), het reglement inzake de raadpleging van gegevens, de jurisprudentie en de secundaire literatuur, zoals Peters en Ludeman.

Artificiële intelligentie

De analyse is normatief juridisch en niet empirisch statistisch. Het gaat om de toetsing van de rechtsstructuur aan de constitutionele beginselen, niet om econometrische effectmeting.

Wat effectiviteitsanalyse betreft: sinds de inwerkingstelling van het reglement inzake de raadpleging van gegevens noteert de Federale Belastingdienst een aanzienlijke stijging van de detectie van niet aangegeven inkomens- en vermogensbestanden. Volgens het jaarverslag van het Duitse Federaal Ministerie van Financiën leidt het systeem tussen 2005 en 2022 tot de identificatie van ongeveer 1,4 miljoen rekeningen

que la proportionnalité individuelle et la transparence soient garanties. D'autres décisions rendues ensuite par diverses juridictions allemandes ont permis d'affiner cette jurisprudence. Celle-ci présente une constance: la Cour des comptes autorise l'échange de données, mais uniquement dans un cadre strict sur le plan de la finalité et de la proportionnalité.

Pas moins de trente audits ont été réalisés en 2022. Dans quatre cas, des manquements mineurs à la procédure ont été constatés. Il s'agissait de journalisations incomplètes ou de notifications tardives. Mais aucun manquement n'a donné lieu à une sanction formelle.

Il existe évidemment des principes méthodologiques de base. L'évaluation exige une double approche. D'une part, il faut examiner dans quelle mesure le système atteint la finalité poursuivie: la lutte contre la fraude fiscale, le blanchiment d'argent et le versement indu d'allocations. D'autre part, il est également nécessaire d'évaluer si ces résultats sont obtenus en respectant les droits fondamentaux. C'est ce juste équilibre entre la lutte contre la fraude et les droits fondamentaux qui doit être garanti: les exigences de proportionnalité, de subsidiarité et de finalité.

Dans la doctrine allemande, cette double approche est souvent décrite comme l'équilibre entre l'efficacité du fisc et la protection des droits fondamentaux. Le Tribunal constitutionnel fédéral a souligné à plusieurs reprises que ces deux dimensions ne doivent pas nécessairement s'opposer et qu'elles peuvent être parfaitement prévisibles et contrôlables moyennant les cadres légaux nécessaires.

Cette analyse repose sur les textes de l'article 24c de la *Kreditwesengesetz* (KWG), de l'article 93 de l'*Abgabenordnung* (AO), du règlement relatif à la consultation des données, ainsi que sur la jurisprudence et la littérature secondaire (notamment des auteurs Peters et Ludeman).

Intelligence artificielle

L'analyse est normative sur le plan juridique et non empirique sur le plan statistique. Il s'agit d'évaluer la structure juridique au regard des principes constitutionnels, et non de mesurer les effets sur le plan économétrique.

En ce qui concerne l'analyse de l'efficacité, l'administration fiscale fédérale observe, depuis l'entrée en vigueur du règlement concernant la consultation de données, une hausse considérable de la détection d'éléments et de revenus non déclarés. Selon le rapport annuel du ministère fédéral allemand des Finances, le système a permis, entre 2005 et 2022, d'identifier environ 1,4 million de comptes qui n'avaient pas été renseignés dans les

die niet in de belastingaangiften waren vermeld. Het aantal zelfstandzigen, vrijwillige rechtszettingen, nam in dezelfde periode met meer dan 40 % toe, wat wijst op een preventieve werking. Het bestaan van het systeem bevordert de analyse.

Het reglement inzake de raadpleging van gegevens wordt dus niet enkel reactief gebruikt, maar heeft ook een afschrikkend en conformerend effect. De BAFin-infrastructuur (de Duitse toezichthouder voor de financiële markten) maakt opvragingen mogelijk binnen seconden, waardoor belastingonderzoeken sneller kunnen worden afgerond, en het Federaal Ministerie van Financiën schat de besparing op personeels- en onderzoekskosten op ongeveer 25 miljoen euro per jaar. De maatregel wordt daarom beschouwd als een van de meest rendabele digitale hervormingen in de Duitse fiscale administratie sinds 2000.

Toepassing buiten de fiscaliteit

Naast de controle en het gebruik door het Federaal Ministerie van Financiën van Duitsland zijn er ook de sociale zekerheidsinstellingen en de justitiële autoriteiten die de procedure gebruiken voor de opsporing van onrechtmatige sociale uitkeringen, faillissementsfraude en ook witwas- en confiscatieonderzoeken. En volgens de Duitse RVA leidt het gebruik in 2021 tot een terugvordering van meer dan 80 miljoen euro aan onrechtmatig uitgekeerde steun.

De effectiviteit in het strafrechtelijke context is moeilijker te kwantificeren, maar de procureur-generaal rapporteerde dat bankidentificatie via het reglement inzake de raadpleging van gegevens in 60 % van de witwasdossiers beslissend was voor de bewijsvoering. Het systeem berust op een hoog automatiseringsniveau en vergt minimale personele tussenkomst.

De kost per opvraging ligt rond 5 euro maar de totale jaarlijkse implantatiekosten (hardware, software, audits) bedragen ongeveer 20 miljoen euro in Duitsland, gedragen door de federale begroting.

Gelet op de extra fiscale ontvangsten wordt de kostenbatenverhouding algemeen als gunstig beschouwd. Zoals in Vlaanderen doet men een MKBA, een maatschappelijke kostenbatenanalyse.

De BAFin benadrukt in zijn jaarverslag in 2022 dat het reglement inzake de raadpleging van gegevens

déclarations fiscales. Le nombre de d'autocorrections et de rectifications spontanées a augmenté de plus de 40 % au cours de la même période, ce qui témoigne de l'effet préventif du dispositif. L'existence du système favorise l'analyse.

Le règlement concernant la consultation des données n'est donc pas seulement utilisé de manière réactive, mais il a également un effet dissuasif et contribue à un meilleur respect des règles. L'infrastructure de la BAFin (l'autorité allemande de surveillance des marchés financiers) permet d'effectuer des consultations en quelques secondes, ce qui accélère les enquêtes fiscales. Le ministère fédéral des Finances estime les économies réalisées en termes de frais de personnel et d'enquête à environ 25 millions d'euros par an. La mesure est dès lors considérée comme l'une des réformes numériques les plus rentables de l'administration fiscale allemande depuis 2000.

Application en dehors du domaine de la fiscalité

Outre l'application à des fins de contrôle et l'utilisation par le ministère fédéral allemand des Finances, les organismes de sécurité sociale et les autorités judiciaires ont également recours à cette procédure pour détecter les allocations sociales indûment versées et les faillites frauduleuses, ainsi que dans le cadre d'enquêtes en matière de blanchiment et de confiscation. Selon l'équivalent allemand de l'ONEM, l'utilisation du système a permis de récupérer plus de 80 millions d'euros d'aides indues en 2021.

L'efficacité dans le contexte pénal est plus difficile à quantifier, mais le procureur général a indiqué que l'identification bancaire par le biais du règlement concernant la consultation de données avait été déterminante pour l'administration de la preuve dans 60 % des dossiers de blanchiment. Le système s'appuie sur un niveau élevé d'automatisation et nécessite une intervention humaine minimale.

Le coût d'une consultation est d'environ 5 euros, mais les frais de mise en œuvre en Allemagne (pour le matériel, les logiciels et les audits) s'élèvent au total à quelque 20 millions d'euros par an, qui sont pris en charge par le budget fédéral.

Compte tenu des recettes fiscales supplémentaires, le rapport coût-bénéfices est généralement considéré comme positif. Une analyse sociale des coûts et des bénéfices est réalisée, à l'instar de ce qui se fait en Flandre.

Dans son rapport annuel de 2022, la BAFin souligne que le règlement concernant la consultation de données

qua technische betrouwbaarheid 99,99 % haalt, met minder dan 0,01 % foutmeldingen. De digitale beveiliging is gebaseerd op encryptie en een meervoudige authenticatiearchitectuur.

Publieksonderzoeken tonen dat ongeveer 70 % van de ondervraagde maatregelen als gerechtvaardigd beschouwd mits beperkt tot fraude- en belastingdoeleinden. Het maatschappelijke draagvlak steunt op de perceptie dat het systeem gerechtvaardigd en niet alomvattend is.

Burgers ervaren geen *Big-Brother*-effect, mede omdat er geen transactiedata worden verwerkt. Wat is dan de grondwettelijke proportionaliteitsanalyse? Het Duitse recht hanteert sinds jaren de viertrapstoets van proportionaliteit. Wettig doel, geschiktheid, noodzakelijkheid en evenredigheid in de enge zin. Deze toets vloeit voort uit artikel 20 van de Grondwet en wordt toegepast telkens wanneer een overheidshandeling een grondrecht, zoals het recht op informatiele zelfbeschikking, beperkt. Het reglement inzake de raadpleging van gegevens wordt op elk van deze vier niveaus onderzocht.

Legitiem doel

Is er sprake van een legitiem doel? Het doel van de maatregel is de handhaving van de fiscale gelijkheid en de doeltreffende inning van belastingen, als ook de bestrijding van witwassen en sociale zekerheidsfraude. Het Hof erkent deze doelstellingen als legitiem, omdat zij rechtstreeks bijdragen aan de bescherming van het algemeen belang en aan de instandhouding van de financiële basis van de Staat. De wetgever heeft bovendien het doel duidelijk en limitatief omschreven in artikel 24c van de *Kreditwesengesetz* (KWG), lid 1, en in artikel 93 van de *Abgabenordnung* (AO), lid 7.

Daarmee is voldaan aan de legaliteits- en verspelbaarheidsvrijheden van artikel 2 van de Grondwet en artikel 8 van het EVRM. De burger kan redelijk voorzien in welke situaties zijn gegevens kunnen worden opgevraagd, wat dus niet het geval is met *money control*.

Geschiktheid

De maatregel is geschikt om de beoogde doelstelling te realiseren, omdat hij de fiscus en andere bevoegde autoriteiten in staat stelt om verborgen bankrelaties te identificeren zonder het bankgeheim volledig op te heffen. De beperking tot inhoudsgegevens werd door het Hof uitdrukkelijk geprezen als een minder ingrijpende vorm van transparantie. Dat is het arrest van 12 juli

atteint een fiabiliteit technische van 99,99 %, met minder dan 0,01 % van signaleringen d'erreur. La protection numérique est basée sur le cryptage et sur une architecture d'authentification multiple.

Des sondages révèlent qu'environ 70 % des personnes interrogées considèrent que les mesures sont justifiées, pour autant qu'elles soient appliquées uniquement aux fins de la lutte contre la fraude et de la taxation. L'adhésion sociale repose sur la perception que le système est légitime et qu'il n'est pas universel.

Les citoyens ne ressentent pas d'effet *Big Brother*, notamment parce qu'il n'y a aucun traitement des données de transactions. En quoi consiste donc le contrôle constitutionnel de proportionnalité? Le droit allemand connaît, depuis des années, le contrôle de proportionnalité en quatre points: objectif légal, adéquation avec l'objectif, nécessité et proportionnalité au sens strict. Ce contrôle découle de l'article 20 de la Constitution et est exercé à chaque fois qu'un acte des pouvoirs publics limite un droit fondamental, tel que le droit à l'autodétermination en matière d'information. Le règlement concernant la consultation de données est évalué à l'aune de chacun de ces quatre critères.

Objectif légitime

L'objectif est-il légitime? La mesure vise à assurer l'égalité fiscale et la perception efficace des impôts, et à lutter contre le blanchiment et la fraude sociale. La Cour constitutionnelle fédérale considère ces finalités comme légitimes, en ce qu'elles contribuent directement à protéger l'intérêt général et à préserver la base financière de l'État. En outre, le législateur a défini l'objectif de manière claire et limitative dans l'article 24c, alinéa 1^{er}, de la loi bancaire allemande (*Kreditwesengesetz* – KWG), ainsi que dans l'article 93, alinéa 7, du code fiscal allemand (*Abgabenordnung* – AO).

La mesure répond ainsi aux exigences de légalité et de prévisibilité définies à l'article 2 de la Constitution et à l'article 8 de la CEDH. Le citoyen peut raisonnablement prévoir dans quelles situations ses données pourront être consultées, ce qui n'est pas le cas dans le cadre du *money control*.

Adéquation

La mesure est en adéquation avec l'objectif visé, en ce qu'elle permet à l'administration fiscale et aux autres autorités compétentes d'identifier des relations bancaires cachées sans lever totalement le secret bancaire. Dans son arrêt du 12 juillet 2007, la Cour a considéré explicitement que la limitation aux données de base des comptes (*Kontenstammdaten*) constituait

2007. Het systeem maakt het bovendien mogelijk om rechtmatige belastingplichtigen te beschermen tegen onnodige controles, aangezien enkel geïdentificeerde risico's worden onderzocht. De geschiktheid wordt dus niet betwist.

Noodzakelijkheid

De noodzakelijkheidstoets vereist dat er geen ander even doeltreffend maar minder ingrijpend middel bestaat. Voorafgaande aan de invoering werden verschillende alternatieven onderzocht, waaronder uitbreiding van de algemene aangifteplicht voor buitenlandse rekeningen, systematische samenwerking met banken op vrijwillige basis of versterking van de maandingsplicht bij specifieke transacties. Het Hof heeft geoordeeld dat deze alternatieven onvoldoende effectief of te afhankelijk waren van vrijwillige medewerking van de belastingplichtigen.

Het reglement inzake de raadpleging van gegevens werd als noodzakelijk maar minimaal intensief beschouwd, juist omdat het geen continue datastroom creëert, de toegang slechts ad hoc en individueel plaatsvindt en de informatie zich beperkt tot identificatie-elementen. Het Hof preciseerde dat de wetgever verplicht is de noodzaak periodiek te herbeoordelen en indien de technologische of administratieve evoluties een lichter middel mogelijk maken, moet de regeling dien overeenkomstig worden aangepast.

Evenredigheid in enge zin

Bij deze vierde stap wordt afgewogen of het voordeel voor het algemeen belang in verhouding staat tot de inbreuk van het grondrecht. Het Hof stelde vast dat de maatregel slechts een beperkt gegevenspakket betreft. De niet-selectieve massasurveillance uitsluit. Dat is hetgeen wat het *money control* wel wil doen.

Het Duitse systeem voorziet bovendien in een strikte logging, bewaartermijnen en een kennisgevingsprocedure. De Duitse federale financiële toezichthouder (BaFin) en de Duitse federale commissaris voor gegevensbescherming en vrijheid van informatie (BFDI) zijn eveneens verplicht om onafhankelijke controles uit te voeren. Ten slotte beschikken burgers over beroepsmogelijkheden.

Deze elementen leiden tot de conclusie dat de beperking aanvaardbaar is binnen een democratische rechtsstaat. Het Hof hanteert de doctrine van de praktische concordantie, het streven naar een evenwicht waarbij beide waarden, gegevensbescherming en belastingrechtvaardigheid, zoveel mogelijk worden verzoend.

une forme de transparence moins intrusive. En outre, le système permet de protéger les contribuables en règle contre les contrôles inutiles, dès lors que seuls les risques identifiés font l'objet d'un examen. L'adéquation de la mesure n'est donc pas contestée.

Nécessité

Le contrôle de la nécessité vise à évaluer s'il n'existe pas de moyen moins intrusif qui soit aussi efficace. Plusieurs autres solutions ont été envisagées avant l'introduction de la mesure: l'extension de l'obligation générale de déclaration pour les comptes étrangers, la coopération systématique avec les banques sur une base volontaire, le renforcement de l'obligation de signalement pour les transactions spécifiques, etc. La Cour a estimé que ces solutions n'étaient pas assez efficaces ou étaient trop tributaires de la coopération volontaire des contribuables.

La Cour a jugé que le règlement concernant la consultation de données était nécessaire tout en étant très peu intrusif, précisément parce qu'il ne crée pas de flux de données continu, que l'accès n'est ouvert que de manière ponctuelle et individuelle, et que l'information se limite aux données d'identification. La Cour a précisé que le législateur était tenu de réévaluer régulièrement la nécessité du système et, le cas échéant, de le modifier si l'évolution technologique ou administrative permettait de recourir à un outil plus discret.

Proportionnalité au sens strict

La quatrième étape de ce contrôle consiste à évaluer si l'avantage pour l'intérêt public est proportionné à la violation du droit fondamental. La Cour a estimé que la mesure ne concerne qu'un ensemble limité de données et qu'elle exclut la surveillance de masse non sélective. C'est en revanche ce que le gouvernement belge entend instaurer au travers du contrôle des flux financiers.

Le système allemand prévoit en outre une journalisation rigoureuse, des délais de conservation ainsi qu'une procédure de notification. L'Autorité fédérale allemande de supervision financière (BaFin) et le commissaire fédéral allemand à la protection des données et à la liberté d'information (BFDI) sont également tenus de procéder à des contrôles indépendants. Enfin, les citoyens disposent de voies de recours.

Il ressort de ces éléments que la limitation du droit à la protection des données est acceptable dans un État de droit démocratique. La Cour applique la doctrine de la concordance pratique, qui vise à trouver un équilibre permettant de concilier autant que possible les deux valeurs que sont la protection des données et la justice

De toets resulteert in de constitutioneel draagsysteem, dat de noodzakelijke doelstelling bereikt met minimale inbreuk op de persoonlijke levenssfeer.

De proportionaliteitsbeoordeling wordt versterkt door drie complementaire beginselen: legaliteit, transparantie en doelbinding.

— *Legaliteit*

De bevoegdheid tot opvraging, moet rechtstreeks uit de wet voortvloeien. Geen delegatie aan uitvoeringsbesluiten of interne richtlijnen is toelaatbaar. Dit volgt uit de voorbehouden van de wet, in het Duitse staatsrecht.

— *Transparantie*

Burgers moeten kunnen nagaan of wanneer en door wie hun gegevens zijn opgevraagd. De kenningsgevingsplicht in artikel 24c van de KWG dient dit doel.

— *Doelbinding*

Gegevens verkrijgen via het reglement inzake de raadpleging van gegevens mogen enkel worden gebruikt voor het doel waarvoor zij zijn verkregen. Secundair gebruik, bijvoorbeeld profilering, is uitdrukkelijk uitgesloten. Het Hof beschouwt deze drie beginselen samen als essentiële randvoorwaarden om de proportionaliteit van het systeem te handhaven.

Het Duitse constitutionele recht past geen absolutistische privacyopvatting toe. In tegenstelling tot wat sommige mensen soms zeggen, dat is niet het geval. Het uitgangspunt is dat het individu deelneemt aan een ordelijke belasting- en rechtssamenleving waarin beperkte transparantie tegenover de Staat rechtvaardigd is om de wederkerigheid van de publieke lasten te waarborgen.

Door de burger levert minimaal informatie aan de Staat. De Staat waarborgt dat deze informatie niet voor andere doeleinden wordt gebruikt. Deze reciproke verklaart waarom het systeem, ondanks zijn intrusieve potentieel, grondwettelijk houdbaar blijft. De *Kontenregister*-wet past binnen het bredere EU-kader voor financiële transparantie. Dat is uitgewerkt in de vierde antiwitwasrichtlijn, 2015/849, in de vijfde anti-witwas Richtlijn 2018/843 en in de Richtlijn 2019/1153, die de toegang van overheidsinstanties tot bankrekeninginformatie regelt.

Artikel 32 van Richtlijn 2015/849 verplicht elke lidstaat een nationaal bankenregister of zoekmechanisme op te

fiscale. La procédure de contrôle atteste de la constitutionnalité du système: l'objectif nécessaire est atteint et l'ingérence dans la vie privée est minimale.

Le contrôle de proportionnalité est renforcé par trois principes complémentaires, à savoir: la légalité, la transparence et la limitation des finalités.

— *Légalité*

Le droit de consultation doit découler directement de la loi. Aucune délégation n'est permise par voie d'arrêtés d'exécution ou de directives internes. Ce droit est en effet réservé à la loi dans le droit constitutionnel allemand.

— *Transparence*

Les citoyens doivent pouvoir vérifier quand et par qui leurs données ont été consultées. L'obligation de notification prévue à l'article 24c de la loi sur le crédit (KWG) poursuit cet objectif.

— *Limitation des finalités*

Les données obtenues en vertu du règlement allemand sur la consultation des données ne peuvent être utilisées qu'aux fins pour lesquelles elles ont été obtenues. Toute utilisation secondaire, par exemple à des fins de profilage, est expressément exclue. La Cour considère ces trois principes comme des conditions préalables essentielles au maintien de la proportionnalité du système.

Contrairement à ce que d'aucuns prétendent parfois, le droit constitutionnel allemand ne s'appuie pas sur une vision absolutiste de la vie privée. Il part du principe que l'individu participe à l'ordre fiscal et juridique dans lequel une transparence limitée vis-à-vis de l'État est justifiée pour garantir la réciprocité des charges publiques.

Le citoyen fournit un minimum d'informations à l'État, qui garantit quant à lui que ces informations ne seront pas utilisées à d'autres fins. Cette réciprocité explique pourquoi le système, malgré son potentiel intrusif, reste constitutionnellement viable. La loi allemande sur le registre des comptes (*Kontenregister*) s'inscrit dans le cadre plus large du système de transparence financière de l'Union européenne. Ce système a été instauré par la quatrième directive anti-blanchiment (2015/849), la cinquième directive anti-blanchiment (2018/843) et la directive (UE) 2019/1153, qui encadre l'accès des autorités publiques aux informations relatives aux comptes bancaires.

L'article 32 de la directive (UE) 2015/849 impose à chaque État membre de mettre en place un registre

zetten dat identificatie van rekeninghouders mogelijk maakt. Dat is de vierde anti-witwas Richtlijn. Tenzij dat België uit de EU stapt, is dat geen optie.

De heer Lode Vereeck (VB) legt uit dat de Vlaams Belangfractie voorstander is van de EEG, waarnaar een eengemaakte markt wordt gestreefd, op economisch en financieel vlak.

De heer Vincent Van Quickenborne (Open Vld) legt uit dat Duitsland die Richtlijn heeft uitgevoerd, maar koos dus voor een gedecentraliseerde implementatie.

De gegevens blijven bij de banken, maar het is via het BAfIN-interface doorzoekbaar. En dat model is door de Europese Commissie meermaals als conforme richtlijn bevestigd, omdat het *functional equivalence* biedt zonder centrale opslag.

Het systeem steunt op artikel 6, lid 1, punt c) en e) van de GDPR. En de wettelijke grondslag is de formele wet, het artikel 24c van de *Kreditwesengesetz* (KWG) en artikel 93 van de belastingwetboek (*Abgabenordnung*, AO).

De Duitse implementatie wordt vaak als voorbeeld genoemd van *GDPR by design*, omdat de doeleinden zijn dus omschreven precies, de verwerking is beperkt tot noodzakelijke gegevens en technische & organisatorische maatregelen zijn structureel ingebouwd. Het Hof van Justitie van de Europese Unie heeft in de arresten *Schrems II* (16 juli 2020) en *La Quadrature du Net* (6 oktober 2020) herhaald dat algemene en ongerichte dataverwerking onverenigbaar is met artikel 7 en 8 van het EU-handvest.

Het reglement inzake de raadpleging van gegevens voldoet aan deze rechtspraak, doordat het geen massale preventieve verlaming inhoudt, maar herrichte toetsbare bevraging.

Wat zijn de risico's van het systeem?

De grootste uitdaging is de verleiding om het systeem uit te breiden naar nieuwe doeleinden. En dat is hetgeen exact wat er in België gebeurt. *Function creep*, de automatische koppeling van die gegevens met vastgoed- of voertuigdossiers of voor gebruik van risicoprofilering. Het Federaal Constitutionele Hof heeft herhaaldelijk gewaarschuwd dat elke taakuitbreiding een nieuwe formele wet

bancaire national ou un mécanisme de recherche permettant l'identification des titulaires de comptes. Tel est ce que prévoit la quatrième directive anti-blanchiment. La Belgique doit donc s'y conformer à moins qu'elle ne quitte l'Union européenne.

M. Lode Vereeck (VB) explique que le groupe Vlaams Belang soutient la CEE, dont l'objectif est la création d'un marché unique, tant sur le plan économique que financier.

M. Vincent Van Quickenborne (Open Vld) explique que l'Allemagne a mis en œuvre cette directive, mais de manière décentralisée.

Les banques conservent les données, qui sont toutefois consultables sur l'interface BAfIN. La Commission européenne a confirmé à plusieurs reprises que ce modèle était conforme à la directive, car il offre une *équivalence fonctionnelle* sans stockage centralisé.

Ce système s'appuie sur l'article 6, paragraphe 1, points c) et e), du RGPD, la base légale étant la loi formelle, en particulier l'article 24c de la loi bancaire (*Kreditwesengesetz* – KWG) et l'article 93 du Code des impôts (*Abgabenordnung*, AO).

Cette mise en œuvre de la directive par l'Allemagne est souvent citée pour illustrer la protection des données *dès la conception*, car les finalités sont décrites avec précision, le traitement est limité aux données nécessaires et des mesures techniques et organisationnelles sont intégrées de manière structurelle. Dans ses arrêts *Schrems II* (16 juillet 2020) et *La Quadrature du Net* (6 octobre 2020), la Cour de justice de l'Union européenne a réaffirmé que le traitement général et non ciblé des données était incompatible avec les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

Le règlement relatif à la consultation des données est conforme à cette jurisprudence, car il ne prévoit pas de collecte massive de données à titre préventif, mais une consultation ciblée et contrôlable.

Quels risques ce système comporte-t-il?

Le défi majeur réside dans la tentation d'étendre ce système au-delà de sa portée initiale. C'est exactement ce qui se passe en Belgique: le glissement de finalité (*function creep*) en vue du couplage automatique de ces données avec des dossiers immobiliers ou automobiles ou de l'identification des profils à risque. La Cour constitutionnelle fédérale a mis en garde, à plusieurs reprises,

vereist en opnieuw aan de proportionaliteitstoets moet worden onderworpen.

Zonder die waarborgen zou het evenwicht tussen efficiëntie en *privacy* snel kunnen kantelen en het systeem evolueren tot een vorm van permanente financiële monitoring, wat grondwettelijk ontoelaatbaar zou zijn. Door de sterke digitalisering groeit het belang van cybersecurity. De Duitse Federale Rekenkamer stelde in 2021 vast dat sommige kleinere spaarbanken verouderde encryptiesoftware gebruikten.

Sinds 2023 schrijft de Duitse toezichthouder voor de financiële markten (BaFin) daarom de TLS 1.3-standaard en multifactorauthenticatie voor bij alle gegevensuitwisselingen. Hoewel tot dusver geen inbreuken zijn vastgesteld, blijft continue technische auditing noodzakelijk. De praktijk toont wel aan dat veel burgers zich niet bewust zijn van het feit dat ze recht hebben op kennisgeving en inzage.

De *Federal Commissioner for Data Protection and Freedom of Information* (BfDI) pleit voor een centraal burgerportaal waar men veilig kan nagaan of er een reglement inzake de raadpleging van gegevens heeft plaatsgevonden. Een dergelijk portaal zou de transparantie versterken en het vertrouwen in de overheid vergroten zonder bijkomende administratieve lasten. De Europese Commissie onderzoekt of nationaal systemen zoals het Duitse kunnen worden geïntegreerd in een pan-Europese register voor justitie- en belastingdoeleinden. Duitsland staat hier principeel terughouden tegenover, want het vreest dat een centrale EU-database moeilijk terrein bevat met de Duitse grondrechtencultuur. De voorkeur blijft uitgaan naar interconnectie van decentrale zoekmechanismen met waarborgen op nationaal niveau.

Wat maakt het Duitse systeem zo goed?

— *De constitutionele duurzaamheid*

Het reglement inzake de raadpleging van gegevens voldoet aan de eisen van het Duitse Grondwet en de GDPR dankzij een formele wettelijke basis, duidelijke doelomschrijving, individuele niet-massale opvragingen en onafhankelijk toezicht. Het systeem belicht de Duitse doctrine van praktische concordantie, fiscale rechtvaardigheid en gegevensbescherming in evenwicht.

que tout élargissement des missions nécessitait une nouvelle loi formelle et devait être soumis à un nouveau contrôle de proportionnalité.

En l'absence de ces garanties, l'équilibre entre l'efficacité et le respect de la vie privée pourrait être rapidement compromis et le système pourrait évoluer vers une forme de contrôle financier permanent, ce qui serait inadmissible à la lumière de la Constitution. La numérisation avancée accroît l'importance de la cybersécurité. En 2021, la Cour fédérale des comptes allemande a constaté que certaines petites banques d'épargne utilisaient des logiciels de cryptage obsolètes.

Depuis 2023, l'autorité allemande de surveillance des marchés financiers (BaFin) impose donc d'appliquer la norme TLS 1.3 et l'authentification multifactorielle dans le cadre de tous les échanges de données. Bien qu'aucune infraction n'ait été constatée à ce jour, un audit technique permanent demeure nécessaire. Les faits révèlent toutefois que de nombreux citoyens ne sont pas conscients de leur droit d'être informés et de consulter leurs données.

Le *Commissaire fédéral à la protection des données et à la liberté d'information* (BfDI) plaide en faveur d'un portail citoyen centralisé permettant de vérifier en toute sécurité si un règlement relatif à la consultation des données a été respecté. Un portail de ce type permettrait d'accroître la transparence et de renforcer la confiance dans les pouvoirs publics sans entraîner de lourdeurs administratives supplémentaires. La Commission européenne examine actuellement la possibilité d'intégrer des systèmes nationaux tels que le système allemand dans un registre paneuropéen à des fins judiciaires et fiscales. L'Allemagne se montre en principe réticente à cet égard, car elle craint qu'une banque de données centrale de l'Union européenne ne soit difficilement compatible avec la culture allemande des droits fondamentaux. Elle continue donc d'accorder sa préférence à l'interconnexion de mécanismes de recherche décentralisés assortis de garanties au niveau national.

Quelles sont les forces du système allemand?

— *La durabilité constitutionnelle*

Le règlement relatif à la consultation des données est conforme aux exigences de la Constitution allemande et du RGPD, dès lors qu'il repose sur une base légale formelle, sur une définition claire des objectifs, sur des demandes individuelles et ciblées ainsi que sur un contrôle indépendant. Ce système incarne la doctrine allemande de l'équilibre entre la concordance pratique, la justice fiscale et la protection des données.

— *Decentralisatie als waarborg*

Door de gegevens bij de banken te laten en de BAfIN enkel als router te gebruiken, wordt de kans op machtsconcentratie en misbruik aanzienlijk verkleind. Deze architectuur vormt een model voor lidstaten die transparantie willen combineren met *privacy*.

— *Transparantie en burgerrecht*

De kennisgevingsplicht en het klachtenrecht zijn onmisbaar voor de legitimiteit. Aanbevolen wordt een digitale infrastructuur te ontwikkelen waarmee burgers *real-time* kunnen nagaan wie gegevens heeft geraadplecht.

— *De technologische evolutie*

Nieuwe technologieën zoals kunstmatige intelligentie en *risicoscoring* kunnen de efficiëntie vergroten, maar vereisen in expliciete nieuwe wettelijke grondslag en voorafgaande proportionaliteitsanalyse. Elke vorm van automatische profilering zou in strijd komen met artikel 22 van de GDPR, tenzij voorzien in de wet en gepaard met een echte menselijke tussenkomst.

— *De internationaal betekenis*

Het Duitse model illustreert dat een lidstaat zowel de EU-verplichtingen in zake transparantie als de nationale *privacy* standaarden kan naleven. Duitsland biedt daarmee een juridisch en technisch referentiemodel voor een evenwichtige aanpak van de verwerking van fiscale gegevens.

Strikt handhaven van de scheiding tussen gegevensbeheer, toezicht en gebruik. Versterkt de middelen van de BfDI voor audits. Verkort de bewaartermijn van stamgegevens tot vijf jaar tenzij wettelijk vereist. Ontwikkelt een burgerportaal voor transparantie. En er zijn ook periodes waarin het verantwoordelijk is conform de technologische evoluties.

Door vast te houden aan de principes van doelbinding, individualiseren en onafhankelijk toezicht, blijft Duitsland trouw aan zijn constitutionele traditie van de informatieve zelfbeschikking. Het model toont dat moderne fiscale controle mogelijk is zonder systematische data-mining of permanente surveillance, een evenwicht dat in de Europese context zelden zo consequent juridisch is uitgewerkt.

— *La décentralisation comme garantie*

En permettant aux banques de conserver les données et en utilisant l'interface BAfIN uniquement comme portail d'accès, le risque de concentration du pouvoir et d'abus est considérablement réduit. Cette architecture constitue un modèle pour les États membres qui souhaitent allier transparence et protection du respect de la vie privée.

— *Transparence et droit des citoyens*

L'obligation de notification et le droit de plainte sont indispensables à la légitimité. Il est recommandé d'élaborer une infrastructure numérique permettant aux citoyens de vérifier en temps réel qui a consulté leurs données.

— *L'évolution technologique*

Les nouvelles technologies, telles que l'intelligence artificielle et la classification des risques, peuvent accroître l'efficacité, mais nécessitent une nouvelle base légale explicite et une analyse préalable de proportionnalité. Toute forme de profilage automatique serait contraire à l'article 22 du RGPD, sauf si elle est prévue par la loi et assortie d'une véritable intervention humaine.

— *La signification internationale*

Le modèle allemand démontre qu'un État membre a tout à fait la possibilité de respecter à la fois les obligations européennes en matière de transparence et les normes nationales qui régissent le respect de la vie privée. L'Allemagne fournit ainsi un modèle de référence sur les plans juridique et technique pour une approche équilibrée du traitement des données fiscales.

Ce modèle s'illustre par son respect strict de la séparation entre la gestion, le contrôle et le traitement des données. De plus, il renforce les moyens mis à la disposition de la BfDI pour les audits. Il réduit également le délai de conservation des données de base à cinq ans, sauf exigence légale contraire. Ce dispositif crée en outre un portail citoyen dédié à la transparence. Enfin, il prévoit la réévaluation périodique de la proportionnalité au regard des évolutions technologiques.

Par son respect des principes de finalité, d'individualisation et d'impartialité du contrôle, l'Allemagne reste fidèle à sa tradition constitutionnelle d'autodétermination informationnelle. Ce modèle démontre qu'un contrôle fiscal moderne est possible sans *data mining* systématique ni surveillance permanente. L'équilibre dont il témoigne s'appuie sur des fondements juridiques dont la cohérence est rarement égalée sur la scène européenne.

Het Oostenrijk model

De Oostenrijkse regeling in zake financiële gegevenscontrole behoort tot de meest verfijnde en constitutionele verantwoorde modellen binnen de Europese Unie. Waar België en enkele andere lidstaten bankregisters onder rechtstreeks beheer van de fiscale administratie plaatsen, koos Oostenrijk bewust voor een neutraal gedepolitiseerd systeem waarin de Oostenrijkse Nationale Bank, optreedt als technisch beheerder van een centrale databank met het sluiten identificatiegegevens van bankrekeningen in de kluis.

Het systeem is in werking getreden op 1 januari 2016. Het vormt het sleutelement van de Oostenrijkse fiscale hervorming na de financiële crisis van 2008 en de daaropvolgende internationale druk op bankgeheimen.

Het systeem tracht de nood aan transparantie en fraudebestrijding te verzoenen met de grondrechtelijke bescherming van financiële *privacy*. De wetgeving werd ontworpen als een evenwicht tussen drie doelstellingen.

— de effectieve uitvoering van anti-witwas en fiscale verplichtingen in overeenkomstig de EU-Richtlijnen;

— de instandhouding van constitutionele waarborgen in zake gegevensbescherming;

— Het behoud van het vertrouwen in het Oostenrijkse financiële systeem. Het Oostenrijkse *Kontenregister- und Konteneinschaugesetz* (KontRegG) is dus een register van rekeningen, niet van transacties.

Dit geeft de autoriteiten een instrument om snel te achterhalen wie waar een rekening heeft, maar verhindert elk gebruik van de gegevens voor *datamining* of *risico-scoring*. Tot 2015 kende Oostenrijk een van de strengste bankgeheimen in Europa, vastgelegd in artikel 38 van de Banksectorwet. De regel verbood kredietinstellingen om enige informatie over klanten te verstrekken, behalve op rechtelijk bevel. De wereldwijde strijd tegen belastingontduiking, geïntensiveerd door de G20 en de OESO, met de invoering van de *Common Reporting Standard*, plaatste Oostenrijk onder toenemende druk.

Le modèle autrichien

La réglementation autrichienne en matière de contrôle des données financières figure parmi les modèles les plus fins et les plus constitutionnellement conformes de l'Union européenne. Alors que la Belgique et d'autres États membres ont placé les registres bancaires sous le contrôle direct de l'administration fiscale, l'Autriche a choisi, quant à elle, un système neutre et dépolitisé au sein duquel la Banque nationale d'Autriche joue le rôle de gestionnaire technique d'une banque de données centrale reprenant les données d'identification des comptes en banque et des coffres.

Ce système est entré en vigueur au 1^{er} janvier 2016 et il représente la clef de voûte de la réforme fiscale mise en place par l'Autriche après la crise financière de 2008 et la pression internationale qu'elle a exercé sur le secret bancaire.

Le système tente de concilier le besoin de transparence et de lutte contre la fraude avec la protection, garantie par la Constitution, de la vie privée financière. La législation a été pensée comme un équilibre entre trois objectifs:

— exécuter efficacement les obligations fiscales et relatives à la lutte contre le blanchiment, conformément aux directives européennes;

— préserver les garanties constitutionnelles en matière de protection des données;

— maintenir la confiance envers le système financier autrichien. Le *Kontenregister- und Konteneinschaugesetz* (KontRegG) autrichien est donc un registre des comptes et pas des transactions.

Les autorités disposent ainsi d'un instrument grâce auquel elles peuvent déterminer rapidement qui possède un compte et à quel endroit. Ce système ne leur permet toutefois pas d'exploiter les données dans le cadre d'une procédure de *data mining* ou d'évaluation du risque que représente un contribuable. Jusqu'en 2015, l'Autriche appliquait l'une des politiques les plus strictes d'Europe en matière de secret bancaire, reposant sur l'article 38 de la loi sur le secteur bancaire. Il était ainsi interdit aux établissements de crédit de communiquer la moindre information au sujet de leurs clients, sauf en cas d'injonction judiciaire. La lutte engagée mondialement contre la fraude fiscale, et dans laquelle se sont pleinement investis le G20 et l'OCDE, avec l'institution du *Common Reporting Standard*, a rendu la position autrichienne de plus en plus inconfortable.

De Europese Commissie beschouwde de Oostenrijkse terughoudendheid als een belemmering voor fiscale samenwerking. In 2014 werd een wet op de wijziging van belastingen aangenomen, die het bankgeheim gedeeltelijk ophief voor fiscale doeleinden.

Daarop volgde de invoering van de *Kontenregister*-wet van 26 juli 2015, dat een kader schiep voor een centraal register van bank- en kluisgegevens. Deze wet kadert binnen de uitvoering van de vierde Europese *Anti-Witwas Richtlijn* 2015/849 en de Richtlijn 2011/16 betreffende de administratieve samenwerking op fiscaal gebied. De bedoeling was om Oostenrijk in lijn te brengen met de internationale transparantienormen zonder afbreuk te doen aan constitutionele *privacy* beschermingen.

Er waren tal van parlementaire debatten. Tijdens de parlementaire behandeling benadrukten meerdere fracties de nood aan evenwicht tussen transparant en vertrouwelijkheid. Het Parlement drong er ook op aan dat het beheer niet bij de Belastingdienst mocht liggen, maar bij een onafhankelijke niet-politieke instelling. Vandaar de keuze voor de Oesterreichische Nationalbank (OeNB).

Wat is de juridische basis en opbouw van het systeem?

De wettelijke grondslag zijn de kernbepalingen van Het Oostenrijkse *Kontenregister- und Konteneinschaugesetz* (KontRegG) die zijn opgenomen in artikelen 1 tot 9 van de *Kontenregister*-wet, de aanvullende bepalingen in het federale belastingwetboek (*Bundesabgabenordnung*, BAO) en de bancaire wet (*Bankwesengesetz*) dat artikel 38, het bankgeheim, aanpaste om Het Oostenrijkse *Kontenregister- und Konteneinschaugesetz* (KontRegG) mogelijk te maken. Er is veel discussie geweest in Oostenrijk om toch het bankgeheim te respecteren en te moduleren. De federale ministerie van Financiën is verantwoordelijk voor het algemene beleid en de wettelijke interpretatie, maar de uitvoering ligt bij de Oostenrijkse Nationaalbank die fungeert als technisch beheerder.

Wat is het doel van het register?

Het gaat dus om een instrument ter ondersteuning van de uitvoering van fiscale, strafrechtelijke en anti-witwas wetten, niet om een permanent toezichtmechanisme.

Wat zijn de gegevenscategorieën en inhoud van het register?

La Commission européenne a vu dans la réticence autrichienne une entrave à la collaboration fiscale. En 2014, une loi relative à la modification des impôts a été adoptée, laquelle levait partiellement le secret bancaire à des fins fiscales.

La loi du 26 juillet 2015 instituant le *Kontenregister* a ensuite été promulguée. Cette loi créait le cadre d'un registre central des données relatives aux comptes bancaires et aux coffres, s'inscrivant ainsi dans l'exécution de la quatrième directive européenne antiblanchiment 2015/849 et de la directive 2011/16 relative à la coopération administrative dans le domaine fiscal. L'objectif était d'aligner l'Autriche sur les normes de transparence internationales sans porter préjudice à la protection, ancrée constitutionnellement, de la vie privée.

Cette évolution législative a suscité un vif débat parlementaire au cours duquel plusieurs groupes ont souligné l'importance du maintien d'un juste équilibre entre la transparence et la confidentialité. Le Parlement s'est également fermement positionné dans un refus de voir la gestion de cette matière confiée à l'administration fiscale. Une institution apolitique et indépendante devait être à la manœuvre. Le choix s'est ainsi porté sur la Banque nationale d'Autriche (*Oesterreichische Nationalbank* – OeNB).

Quelle est la base juridique de ce système et comment est-il conçu?

La base légale est constituée par les dispositions centrales du *Kontenregister- und Konteneinschaugesetz* (KontRegG) autrichien, qui figurent aux articles 1 à 9 de la loi sur le *Kontenregister*, tandis que les dispositions complémentaires sont reprises dans le code fiscal fédéral (*Bundesabgabenordnung* – BAO) et dans la loi bancaire (*Bankwesengesetz*), qui a modifié l'article 38, sur lequel reposait le secret bancaire, afin de permettre la création du *Kontenregister- und Konteneinschaugesetz* (KontRegG) autrichien. L'idée de maintenir et de moduler le secret bancaire a fait l'objet de nombreuses discussions en Autriche. Le ministère fédéral des Finances est chargé de la politique générale et de l'interprétation légale, mais la compétence d'exécution relève de la Banque nationale d'Autriche, qui intervient en qualité de gestionnaire technique.

Quel est l'objectif du registre?

Il s'agit donc d'un instrument destiné à faciliter la mise en œuvre des lois fiscales, pénales et anti-blanchiment, et non d'un mécanisme de surveillance permanent.

Quelles sont les catégories de données et quel est le contenu du registre?

Het register bevat uitsluitend identificatiegegevens, zoals naam, adres en geboortedatum van de rekeninghouder, het rekeningnummer, de naam van de bank, de openings- en sluitingsdatum van de rekening, de namen van eventuele gevolmachtigden, de type rekening (zicht, spaar, effectrekening of kluis). De wet verbiedt expliciet het opnemen van saldie, van de transactiegeschiedenis en van renteinkomsten of vermogensgegevens. De gegevens worden dagelijks door de banken elektronisch overgemaakt aan de OeNB via een beveiligd netwerk. De banken blijven verantwoordelijk voor de juistheid van de data, de OeNB voor de technische integriteit van het register.

Wat is de rol van de Oesterreichische Nationalbank (OeNB)?

Het is een onafhankelijke instelling van publiek recht, die in dit geval optreedt als verwerker onder toezicht van het Federaal Ministerie van Financiën, die beheert de IT-infrastructuur, bewaart de gegevens en waarborgt de beveiliging volgens de ISO 27.001-normen. De OeNB heeft geen toegang tot de nodige gegevens. Enkel bevoegde autoriteiten kunnen via een beveiligde elektronische aanvraag informatie opvragen.

Wie zijn de bevoegde instanties?

De volgende instanties kunnen toegang krijgen tot het register: de fiscale administratie de douane, het Openbaar Ministerie, de criminele politie en de meldingsinstantie voor witwassen (A-FIU, de officiële benaming van de Oostenrijkse Financial Intelligence Unit). Elke instantie heeft een eigen toegangskanaal met authenticatie via elektronische certificaten. De Oostenrijkse gegevensbeschermingsautoriteit oefent onafhankelijk toezicht uit op alle verwerkingen. Ze beschikt over onderzoeks- en sanctiebevoegdheden.

De Oostenrijkse gegevensbeschermingsautoriteit voert jaarlijks audits uit bij de OeNB en kan binnen de richtlijnen uitvaardigen over gegevensbescherming.

Hoe loopt de aanvraag?

Elke bevraging van het register verloopt via een digitale interface.

De bevoegde autoriteit dient een aanvraag in met een duidelijke motivering, bijvoorbeeld een identificatienummer of een fiscaal dossier. De aanvraag wordt automatisch geregistreerd en doorgestuurd naar de OeNB. De OeNB

Le registre contient uniquement des données d'identification, comme le nom, l'adresse et la date de naissance du titulaire du compte, le numéro de compte, le nom de la banque, les dates d'ouverture et de clôture du compte, les noms des éventuels mandataires, le type de compte (compte courant, compte d'épargne, compte-titres ou coffre-fort). La loi interdit explicitement l'enregistrement des soldes, de l'historique des transactions et des revenus d'intérêts ou des données patrimoniales. Les données sont transmises quotidiennement par les banques à l'OeNB, au travers d'un réseau électronique sécurisé. Les banques restent responsables de l'exactitude des données, tandis que l'OeNB est responsable de l'intégrité technique du registre.

Quel est le rôle de la Banque nationale autrichienne (OeNB)?

Il s'agit d'un organisme indépendant de droit public qui, en l'espèce, est chargé du traitement des données sous le contrôle du ministère fédéral des Finances, gère l'infrastructure informatique, conserve les données et garantit la sécurité conformément aux normes ISO 27.001. L'OeNB n'a pas accès aux données nécessaires. Seules les autorités compétentes peuvent demander des informations en introduisant une demande électronique sécurisée.

Quelles sont les autorités compétentes?

Les autorités suivantes peuvent accéder au registre: l'administration fiscale, les douanes, le ministère public, la police criminelle et l'autorité de déclaration en matière de blanchiment d'argent (A-FIU, nom officiel de la cellule de renseignement financier autrichienne). Chaque autorité dispose de son propre canal d'accès avec authentification par certificats électroniques. L'autorité autrichienne de protection des données exerce un contrôle indépendant sur tous les traitements. Elle dispose de pouvoirs d'enquête et de sanction.

L'autorité autrichienne de protection des données effectue des audits annuels auprès de l'OeNB et peut émettre des directives en matière de protection des données.

Comment se déroule la demande?

Chaque consultation du registre s'effectue au moyen d'une interface numérique.

L'autorité compétente introduit une demande clairement motivée, en renseignant par exemple un numéro d'identification ou un dossier fiscal. La demande est automatiquement enregistrée et transmise à l'OeNB, qui vérifie ensuite la compétence de l'auteur de la demande,

controleert de bevoegdheid en de volledigheid van de aanvraag en de wettelijke grondslag.

Is het een fiscale, een strafrechtelijke of een AML-context, elke stap wordt gelogd met datum, tijd, instantie en doel. De logbestanden worden gedurende vijf jaar bewaard voor auditdoeleinden. Na goedkeuring ontvangt de aanvrager een gestructureerd elektronisch antwoord met betrokken banken, het rekeningnummer en de identificatie van de titularis. De OeNB levert geen ruwe data of directe toegang tot het register. De gegevens worden enkel vrijgegeven na een specifieke aanvraag.

Meerdere lagen van bescherming voor burgers

Ten eerste is er de kennisgevingsplicht. Volgens artikel 6 van Het Oostenrijkse *Kontenregister- und Konteneinschaugesetz* (KontRegG) moeten betrokkenen na afroep van het onderzoek op de hoogte worden gesteld van het feit dat zijn gegevens werden geraadpleegd tenzij dit het onderzoek zou schaden. Deze kennisgeving moet de instantie zelf doen, niet de OeNB.

Ten tweede is het recht op inzagencorrectie. De burger kan zich rechtstreeks tot de OeNB wenden voor informatie over of zijn gegevens in het register voorkomen en welke instellingen toegang hebben gehad. Fouten moeten binnen 14 dagen worden rechtgezet door de betrokken bank.

De rechtsmiddel

Indien een burger meent dat zijn gegevens onrechtmatig zijn verwerkt, kan hij klacht indienen bij de gegevensbeheerder (artikel 24) en ook eventueel beroep aantekenen bij Het Federaal Administratief Hof om een schadeverhouding te vorderen, op grond van artikel 82 van de GDPR. Het institutioneel toezicht gebeurt in de eerste plaats door de gegevensbeschermingsautoriteit (DSB). De DSB publiceert jaarlijks een verslag over haar toezicht op het Oostenrijkse *Kontenregister- und Konteneinschaugesetz* (KontRegG). De rapporten tonen aan dat het systeem nauwelijks misbruik kent en de procedures strikt worden nageleefd. De meeste incidenten betreffen administratieve fouten, geen inhoudelijke overtredingen.

De Oostenrijkse Rekenkamer controleert periodiek de efficiëntie en kosteneffectiviteit van het register. In zijn verslag van 2019 stelde hij dat het systeem een efficiënt en rechtsstaatelijk gewaarborgden is dat sluit misbruik door zijn structuur uit. Er is ook de interne controle bij de Oesterreichische Nationalbank (OeNB).

l'exhaustivité de celle-ci ainsi que la base légale sur laquelle elle repose.

Qu'il s'agisse d'un dossier fiscal, pénal ou de blanchiment d'argent, chaque étape est consignée en précisant la date, l'heure, l'instance et l'objectif. Les fichiers journaux sont conservés pendant cinq ans à des fins d'audit. Une fois la demande approuvée, le demandeur reçoit une réponse électronique structurée indiquant les banques concernées, le numéro de compte et l'identité du titulaire. L'OeNB ne fournit pas de données brutes ni d'accès direct au registre. Les données ne sont divulguées qu'à la suite d'une demande spécifique.

Plusieurs niveaux de protection pour les citoyens

Il y a d'abord l'obligation de notification. Conformément à l'article 6 de la loi autrichienne sur le registre des comptes et la consultation des comptes (KontRegG), les personnes concernées doivent être informées, après la demande d'enquête, que leurs données ont été consultées, sauf dans l'hypothèse où cette notification nuirait à l'enquête. Cette notification doit être effectuée par l'autorité elle-même, et non par l'OeNB.

Ensuite, le citoyen a le droit d'avoir accès à ses données. Il peut s'adresser directement à l'OeNB pour obtenir des informations sur la présence de ses données dans le registre et sur les institutions qui y ont eu accès. Les erreurs doivent être corrigées dans les quatorze jours par la banque concernée.

Le recours

Si un citoyen estime que ses données ont été traitées de manière illicite, il peut introduire une réclamation auprès du responsable du traitement (article 24) et éventuellement un recours auprès de la Cour administrative fédérale pour demander une indemnisation, sur la base de l'article 82 du RGPD. Le contrôle institutionnel est assuré en premier lieu par l'autorité autrichienne de protection des données (DSB). La DSB publie chaque année un rapport sur son contrôle de l'application de la loi autrichienne relative au registre des comptes et la consultation des comptes (KontRegG). Les rapports montrent que les abus sont rares et que les procédures sont strictement respectées. La plupart des incidents concernent des erreurs administratives, et non des infractions matérielles.

La Cour des comptes autrichienne effectue périodiquement un contrôle de l'efficacité et du rapport coût-bénéfice du registre. Dans son rapport de 2019, elle a indiqué que le système était efficace et conforme à l'état de droit, et que sa structure excluait tout abus. Un contrôle interne est aussi effectué au sein de la Banque nationale autrichienne.

Binnen de OeNB is een aparte afdeling “centrale registerdiensten” opgericht die verantwoordelijk is voor beveiliging, logging en compliance. De OeNB is ISO 27.001 gecertificeerd (ISO 27.001 is een ISO-standaard voor informatiebeveiliging) en onderwerpt zich aan een jaarlijkse penetratietest.

De grondwettelijke verankering

De Oostenrijkse grondwet kent een eigen grondrecht op gegevensbescherming opgenomen in artikel 1 van het DSG. Elke beperking van het recht vereist een wettelijke grondslag in de formele wet, een legitiem doel en de evenredigheid.

Het KontRegG voldoet aan deze criteria, want het is een formele wet, aangenomen door het Parlement in Oostenrijk. Het dient een legitiem doel: het is een fiscale en justitiële transparantie. Het is beperkt tot identificatiegegevens. Het voorziet kennisgeving, inzage en toezicht. Het Oostenrijks Constitutionele Hof (*Verfassungsgerichtshof*), heeft tot dusver geen enkele bepaling van het Oostenrijkse *Kontenregister- und Konteneinschaugesetz* (KontRegG) vernietigd of grondwettelijk problematisch verklaard.

Het KontRegG is volledig in overeenstemming met de vierde en de vijfde anti-witwas Richtlijnen, de GDPR, met name artikelen 6, 22 en 23, en de Richtlijn 2019/1153 betreffende de toegang van bevoegde autoriteiten tot financiële informatie. Oostenrijk heeft het principe van doelbeperking strikt geïncorporeerd. De gegevens mogen enkel worden gebruikt voor fiscale, strafrechtelijke en AML (anti-witwassen) doeleinden.

Heranalyse, profilering of koppeling met andere databanken is verboden zonder nieuwe wet. Sinds de inwerking in 2016 zijn er jaarlijks ongeveer 300.000 raadplegingen. Via het register, hoofdzakelijk door de fiscale administratie en justitie, en volgens het jaarverslag van de OeNB bedraagt de gemiddelde responstijd minder dan twee seconden. Er worden geen systematische datalekken vastgesteld. Het register heeft bewezen zeer efficiënt te zijn in de opsporing van verborgen activa bij fraudeonderzoeken zonder structurele privacyproblemen.

Wel het systeem overwegend positief wordt geëvalueerd, bestaan er toch kritische bedenkingen:

— de centralisatie bij de Oesterreichische Nationalbank (OeNB) schept theoretisch een *single point of failure*. Sommige organisaties, zoals *Epicenter Works*, bekritisseren het gebrek aan publieke transparantie over het aantal opvragingen. Er is geen expliciete verplichting

Une section distincte baptisée “services du registre central” a été créée au sein de l’OeNB. Elle est chargée de la sécurité, de la journalisation et de la conformité. L’OeNB est certifiée ISO 27.001 (norme ISO relative à la sécurité de l’information) et se soumet à un test d’intrusion annuel.

L’ancrage constitutionnel

La Constitution autrichienne reconnaît un droit fondamental propre à la protection des données, inscrit à l’article 1^{er} du DSG. Toute limitation de ce droit requiert une base légale prévue par une loi formelle, un objectif légitime et le respect du principe de proportionnalité.

Le *KontRegG* satisfait à ces critères, puisqu’il s’agit d’une loi formelle adoptée par le Parlement autrichien. Il poursuit un objectif légitime: assurer la transparence fiscale et judiciaire. Sa portée est limitée aux données d’identification. Il prévoit notification, accès consultation et contrôle. La Cour constitutionnelle autrichienne (*Verfassungsgerichtshof*) n’a jusqu’à présent annulé aucune disposition du *KontRegG* ni soulevé une quelconque inconstitutionnalité.

Le *KontRegG* est pleinement conforme aux quatrième et cinquième directives anti-blanchiment, au RGPD, notamment à ses articles 6, 22 et 23, ainsi qu’à la directive 2019/1153 relative à l’accès des autorités compétentes aux informations financières. L’Autriche a strictement intégré dans sa législation le principe de limitation de la finalité. Les données ne peuvent être utilisées qu’à des fins fiscales, pénales et de lutte contre le blanchiment d’argent.

La réanalyse, le profilage et le couplage avec d’autres banques de données sont interdits à défaut d’une nouvelle loi. Depuis l’entrée en vigueur en 2016, environ 300.000 consultations ont lieu chaque année dans le registre. Celles-ci sont effectuées principalement par l’administration fiscale et la justice, et selon le rapport annuel de l’OeNB, le temps de réponse moyen est inférieur à deux secondes. Aucun incident systématique de fuite de données n’a été constaté. Le registre s’est révélé très efficace pour détecter des actifs dissimulés dans le cadre d’enquêtes pour fraude, sans poser de problème structurel en matière de protection de la vie privée.

Bien que le système soit globalement évalué positivement, certaines critiques subsistent:

— la centralisation auprès de l’OeNB crée théoriquement un *point de défaillance unique*. Certaines organisations, telles qu’*Epicenter Works*, critiquent le manque de transparence publique concernant le nombre de demandes de consultation. Il n’existe pas d’obligation

tot voorafgaande rechtelijke machtiging in fiscale zaken, wel in strafzaken.

— de kennisgevingplicht wordt niet altijd efficiënt nageleefd wegens uitzonderingen voorzien in de wet artikel 6, lid 3 van de EVRM.

Toch blijft het algemene oordeel van academische en toezichthoudende instellingen positief. Het systeem houdt als een *best practice* binnen de EU. De Oostenrijkse *Kontenregister-wet* creëert een model dat efficiëntie combineert met rechtsstatelijke waarborgen, centrale opslag koppelt aan neutrale beheersing, transparantie waarborgt doorlogging en toezicht en profilering en datamining expliciet verbiedt.

Het is dus sterker dan het systeem in België, omdat de uitvoerende macht geen directe toegang heeft, de beheerder technisch onafhankelijk is, elke raadpleging getraceerd, verantwoord en controleerbaar is en burgers recht hebben op kennisgeving en inzaam. Waar België met *money control* een stap zet richting algoritmische analyse, handhaaft Oostenrijk de traditionele scheiding tussen informatievoorziening en informatieanalyse. Dit onderscheid is niet louter technisch, maar fundamenteel juridisch.

Het bepaald of financiële controle een administratief hulpmiddel blijft, dat is wel een instrument van preventieve surveillance.

Wat is de praktische werking, wat zijn de waarborgen en de vergelijking met België? Hoe functioneert het *Kontenregister- und Konteneinschaugesetz* (KontRegG) gezet in de praktijk en welke waarborgen zijn er geconcretiseerd?

Het Oostenrijkse systeem houdt internationaal als een voorbeeld van geregleerde financiële transparantie. Het combineert het centraal register met robuuste waarborgen voor rechtsbescherming en gegevensbeveiliging. Daarbij is vooral de rolverdeling tussen overheid en beheerder cruciaal. De fiscale administratie gebruikt het systeem, maar beheert het niet. De OeNB beheert het, maar gebruikt het niet. Dit model van gescheiden functies is fundamenteel anders dan het CAP in België. Dat wordt beheerd door de Nationale Bank en gebruikt door de FOD Financiën. De toegang tot het register verloopt volledig digitaal, via een *web-service*, architectuur die in samenwerking met de OeNB en de *BundesrechnungszentrumKompetenzzentrum für Digitalisierung* (BRZ), wordt ontwikkeld. Elke bemoeide

explicite d'obtenir une autorisation judiciaire préalable en matière fiscale, contrairement à ce qui est prévu pour les affaires pénales.

— l'obligation de notification n'est pas toujours respectée efficacement en raison des exceptions prévues par la loi (article 6, alinéa 3 du *KontRegG*).

L'appréciation générale des milieux académiques et des autorités de contrôle reste toutefois positive. Le système est considéré comme une bonne pratique au sein de l'Union européenne. La *Kontenregister-wet* autrichienne crée un modèle qui associe efficacité et garanties inhérentes à l'état de droit, associe le stockage centralisé à une gestion neutre, assure la transparence par la journalisation et le contrôle, et interdit explicitement le profilage et l'exploration de données (*data mining*).

Ce système est donc plus robuste que le système belge, car le pouvoir exécutif ne bénéficie pas d'un accès direct, le gestionnaire est techniquement indépendant, chaque consultation est tracée, justifiée et contrôlable, et les citoyens ont le droit de recevoir des notifications et d'avoir accès à leurs données. Alors qu'avec *money control*, la Belgique fait un pas dans la voie de l'analyse algorithmique, l'Autriche maintient la séparation traditionnelle entre la fourniture d'informations et l'analyse de l'information. Cette distinction n'est pas seulement technique: il s'agit aussi d'une distinction en matière juridique.

Elle permet de déterminer si le contrôle financier reste un outil administratif ou s'il devient un instrument de surveillance préventive.

Quelle est la mise en œuvre pratique, quelles sont les garanties et quelle la comparaison avec la Belgique peut-elle être faite? Comment fonctionne le *Kontenregister- und Konteneinschaugesetz* (KontRegG) en pratique et quelles garanties ont-elles été concrétisées?

Le système autrichien est reconnu internationalement comme un exemple de transparence financière régulée. Il combine le registre central avec des garanties robustes en termes de protection juridique et de sécurisation des données. À cet égard, la répartition des rôles entre les pouvoirs publics et le gestionnaire est particulièrement essentielle. L'administration fiscale utilise le système, mais ne le gère pas. L'OeNB le gère, mais ne l'utilise pas. Ce modèle de fonctions séparées diffère fondamentalement du PCC en Belgique, qui est géré par la Banque nationale et utilisé par le SPF Finances. L'accès au registre est entièrement numérisée au travers d'un *web-service*, une architecture développée en collaboration avec l'OeNB et le *Bundesrechnungszentrum – Kompetenzzentrum für Digitalisierung* (BRZ). Chaque autorité concernée (fisc,

instantie (fiscus, justitie, politie of de meldingsinstantie voor witwassen (A-FIU)), beschikt over een gecertificeerde elektronische identiteit waarmee ze de aanvragen kunnen indienen.

Elke aanvraag bevat:

— De wettelijke basis van de raadpleging, bijvoorbeeld artikel 38a van de *Bundesabgabenordnung* (BAO) of artikel 116 van de *Strafprozessordnung*;

— De identificatie van de persoon/rechtspersoon;

— De motivering van de noodzaak;

— Het dossiernummer.

De OeNB controleert automatisch bevoegdheid en volledigheid van het verzoek. Indien conform, wordt de vraag doorgestuurd en volgt een elektronisch antwoord binnen enkele seconden. De autoriteit krijgt enkel te zien welke banken een rekening of kluis hebben voor die persoon, niet meer: het is dus gewoon ja of nee.

Elke raadpleging wordt vastgelegd in drie afzonderlijke logsbestanden: de aanvraagde instantie, de OeNB zelf en bij het Federaal Rekencentrum (als neutrale auditbuffer). De logs vermelden datum, uur, instantie, rechtsgrond, referentienummer en technische identificatie. Die gegevens worden gedurende vijf jaar bewaard en kunnen op verzoek van de databasebeheerder of van het Rekenhof worden gecontroleerd.

Deze uitgebreide logging maakt misbruik *a posteriori* detecteerbaar. Oostenrijk is dus niet voor preventieve *datamining*, maar voor een *ex post* controle. Volgens het jaarverslag van OeNB, worden jaarlijks tussen de 250.000 en 350.000 raadplegingen uitgevoerd, voornamelijk door de fiscale administratie. Deze cijfers tonen aan dat efficiëntie en grondrechtelijke waarborgen perfect combineerbaar zijn. Het register is dus niet traag of omslachtig, een argument dat in België soms tegen striktere procedures wordt aangehaald.

Wat zijn de rechten van betrokken burgers in Oostenrijk?

Er is een kennisgevingsplicht. In Oostenrijk is het zo dat artikel 6 van de wet zegt dat wanneer een overheidsdienst gegevens uit het register heeft opgevraagd, de

justice, police ou autorité de déclaration en matière de blanchiment – A-FIU) dispose d'une identité électronique certifiée lui permettant d'introduire des demandes.

Chaque demande contient:

— La base légale de la consultation, par exemple l'article 38a du Code fédéral des impôts (*Bundesabgabenordnung* – BAO) ou l'article 116 du Code de procédure pénale (*Strafprozessordnung*);

— L'identification de la personne physique ou morale;

— La motivation de la nécessité;

— Le numéro de dossier.

L'OeNB contrôle automatiquement si la demande a été introduite par une autorité compétente et si elle est exhaustive. Si la demande est conforme, elle est transmise et une réponse électronique est fournie en quelques secondes. Celle-ci indique uniquement quelles sont les banques qui détiennent un compte ou un coffre-fort au nom de cette personne – rien de plus: la réponse se limite à "oui" ou "non".

Chaque consultation est enregistrée dans trois fichiers journaux distincts: celui de l'autorité requérante, celui de l'OeNB elle-même et celui du Centre fédéral des comptes (*Bundesrechnungszentrum*), qui font office de tampon neutre pour l'audit. Les journaux indiquent la date, l'heure, l'autorité, la base légale, le numéro de référence et l'identification technique. Ces données sont conservées pendant cinq ans et peuvent être vérifiées à la demande du gestionnaire de données ou de la Cour des comptes.

Cette journalisation détaillée permet de détecter les abus *a posteriori*. L'Autriche ne pratique donc pas le *data mining* préventif, mais exerce un contrôle *ex post*. Selon le rapport annuel de l'OeNB, entre 250.000 et 350.000 consultations sont effectuées chaque année, principalement par l'administration fiscale. Ces chiffres montrent que l'efficacité et les garanties fondamentales sont parfaitement compatibles. La procédure basée sur ce registre n'est donc ni lente ni fastidieuse, un argument parfois avancé en Belgique contre l'adoption de procédures plus strictes.

Quels sont les droits des citoyens concernés en Autriche?

Il y a une obligation de notification. En Autriche, l'article 6 de la loi prévoit que lorsqu'un service public a consulté des données dans le registre, les personnes

betrokkenen na afloop van het onderzoek geïnformeerd worden. In België moet je zelf op zoek gaan naar wie heeft er u gelogd. De kennisgeving bevat de volgende informatie: de instantie die de gegevens heeft opgevraagd, de wettelijke basis, de datum van de raadpleging en de mogelijkheid tot bezwaar.

De kennisgeving mag enkel worden uitgesteld als de openbaarmaking het onderzoek zou schaden of de veiligheid van derden in gevaar zou brengen. Zodra het dossier is afgesloten, moet ze alsnog worden bezorgd. Deze bepaling vertelt het principe van transparantie na gebruik, dat in de Oostenrijkse rechtsleer als een *post-factum* controlerecht wordt beschouwd.

Elke burger kan zich rechtstreeks tot de OeNB wenden om te weten of zijn gegevens in het register voorkomen. De OeNB mist het recht op inzaamcorrectie. De OeNB is verplicht om binnen de 14 dagen te antwoorden en eventuele onjuistheden te corrigeren, in overleg met de betrokken bank. Het recht op inzage haalt onafhankelijk van het bestaan van het onderzoek. Dit sluit aan bij artikel 15 van de GDPR en artikel 1 van de Oostenrijkse wet inzake gegevensbescherming.

In de praktijk worden jaarlijks enkele honderden inzageverzoeken ingediend waarvan het merendeel betrekking heeft op technische fouten. Bijvoorbeeld: iemand is twee keer geregistreerd.

Het derde recht als burger is recht op klacht aan beroep. Een burger die meent dat zijn gegevens onrechtmatig zijn verwerkt, kan een klacht indienen bij de gegevensbeschermingsbeheerder (DSB). Een burger kan beroep aantekenen bij het Federaal Administratief Hof en zelfs cassatie instellen bij het Administratief Gerechtshof. De Datenschutzbehörde (DSB), de toezichthouder, kan boetes opleggen aan de OeNB of aan verantwoordelijke autoriteiten die hun kennisgevingsplicht niet naleven.

Er zijn ook waarborgen tegen misbruik.

De doelbinding: het KontRegG, de wetgeving, artikel 1, beperkt het gebruik van het register tot drie doeleinden.

De uitvoering van de fiscale wetgeving, de belastingvoorschriften, de handhaving van de strafprocesordening, het strafrecht en de toepassing van de wetgeving inzake het witwassen van geld.

Elk ander gebruik, bijvoorbeeld voor beleidsanalyse, onderzoek of statistiek, is verboden zonder nieuwe wet.

concernées doivent en être informées à l'issue de l'enquête. En Belgique, les citoyens concernés doivent, quant à eux, vérifier eux-mêmes qui a consulté leurs données. La notification porte sur les informations suivantes: l'autorité ayant procédé à la consultation, la base légale, la date de la consultation et la possibilité d'introduire une réclamation.

La notification ne peut être reportée que si la publication risque de compromettre l'enquête ou la sécurité de tiers. Elle doit néanmoins avoir lieu dès que le dossier est clôturé. Cette disposition énonce le principe de transparence après utilisation des données, reconnu dans la doctrine autrichienne comme un droit de contrôle *ex post*.

Chaque citoyen peut s'adresser directement à l'OeNB pour vérifier si ses données figurent dans le registre. L'OeNB ne dispose pas d'un droit de correction. Elle est toutefois tenue de répondre dans un délai de 14 jours et de corriger toute éventuelle erreur en concertation avec la banque concernée. Le droit d'accès s'exerce indépendamment de l'existence d'une enquête, conformément à l'article 15 du RGPD et à l'article 1^{er} de la loi autrichienne sur la protection des données personnelles.

En pratique, quelques centaines de demandes d'accès sont déposées chaque année, la plupart portant sur des erreurs techniques, comme un double enregistrement.

Le troisième droit du citoyen est le droit de recours. Celui qui estime que ses données ont été traitées de manière illicite peut introduire une réclamation auprès du responsable de la protection des données (DSB). Il peut également faire appel auprès de la Cour fédérale administrative et, le cas échéant, saisir la Cour administrative d'appel d'un recours en cassation. L'autorité de protection des données (*Datenschutzbehörde* – DSB), qui est l'autorité de contrôle, peut infliger des amendes à l'OeNB ou aux autorités responsables ne respectant pas leur obligation de notification.

Il existe également des garanties contre les abus.

La limitation des finalités: l'article 1^{er} de la KontRegG limite l'utilisation du registre à trois finalités.

La mise en œuvre de la législation fiscale et des obligations fiscales, le respect de la procédure pénale et du droit pénal et l'application de la législation relative au blanchiment d'argent.

Toute autre utilisation, par exemple à des fins d'analyse politique, de recherche ou de statistiques, est

Deze strikte doelbinding beantwoordt rechtstreeks aan het artikel 5, eerste lid, b van de GDPR.

Het verbod op profilering en *datamining*: er bestaat een expliciet verbod ingeschreven aan artikel 3, lid 3. Als die even zouden worden gebruikt voor profilering is dat onwettig. Dus Oostenrijk doet net het omgekeerde van datgene wat België doet: wij schrijven in dat het mogelijk is, zij sluiten het effectief uit. Dit verbod sluit elke vorm van *money control* of georganiseerde risicoselectie uit. Autoriteiten mogen geen algoritmes ontwikkelen die profielen van mogelijke fraudeurs genereren. Elke aanvraag moet individueel gemotiveerd of menselijk beoordeeld zijn. Dat is een functionele scheiding.

Het Oostenrijkse model berust op een institutionele en functionele scheiding. De OeNB beheert de data, maar heeft geen bevoegdheid om ze te gebruiken. De fiscale administratie gebruikt ze, maar heeft geen bevoegdheid om ze te beheren. Deze scheiding vormt een structurele waarborg tegenover elkaar. De Belgische situatie is precies omgekeerd. De Nationale Bank is tegelijkertijd beheerder van het uitvoeren van de opvraag in de opdracht van de FOD Financiën, wat het risico op functionele verstrengeling verhoogt.

Ook in Oostenrijk gebeuren er jaarlijks periodieke evaluatierapporten over de naleving van de regels. De DSB bekritiseerde wel dat sommige kennisgeving te laat werden uitgevoerd en riep tot meer automatisering van de melding aan burgers. Het Duitse probleem bestaat dus ook in Oostenrijk.

De rapporten wijzen op een stabiele technische werking en minimale foutenmarge. Het IT-systeem voldoet aan de ISO 27.001 en de BSI-ITveiligheidsnormen (BSI IT-Grundschutz-Standards).

Er is ook een parlementaire opvolging. Het Oostenrijks Rekenhof en de commissie voor Financiën, houden toezicht op de efficiëntie en de proportionaliteit. In 2021 ziet de Oostenrijkse wetgever het systeem als afgrond en voldoende performant, maar zonder verder automatisering of *datamining*. Sinds de invoering van het systeem heeft de Oostenrijkse fiscus meer dan 1 miljard euro aan belastingen al gerecupereerd en de doorlooptijd van fiscale onderzoeken met 40 % verkort.

Toch is het register geen opsporingsinstrument aan zich. Het levert enkele informatie over de locatie van de rekeningen, waarna verder stappen via klassieke

interdite sans nouvelle loi. Cette stricte limitation de la finalité répond directement à l'article 5, paragraphe 1^{er}, b), du RGPD.

L'interdiction du profilage et du *data mining*: une interdiction explicite est prévue à l'article 3, alinéa 3. Si les données devaient être utilisées à des fins de profilage, ce serait illégal. L'Autriche fait donc exactement l'inverse de la Belgique: nous disposons que le profilage est possible, tandis que l'Autriche l'exclut explicitement. Cette interdiction exclut toute forme de *money control* ou de sélection organisée des risques. Les autorités ne peuvent pas développer des algorithmes générant des profils de fraudeurs potentiels. Chaque demande doit être motivée individuellement ou évaluée par un être humain. Il s'agit d'une séparation fonctionnelle.

Le modèle autrichien repose sur une séparation institutionnelle et fonctionnelle. La Banque nationale autrichienne (OeNB) gère les données, mais n'a pas le pouvoir de les utiliser. L'administration fiscale les utilise, mais n'a pas le pouvoir de les gérer. Cette séparation constitue une garantie structurelle de part et d'autre. La situation belge est exactement l'inverse: la BNB gère et exécute à la fois la demande pour le compte du SPF Finances, ce qui augmente le risque d'imbrication fonctionnelle.

En Autriche également, des rapports d'évaluation périodiques sur le respect des règles sont publiés chaque année. La DSB a toutefois critiqué le fait que certaines notifications avaient été effectuées trop tardivement et a appelé à une plus grande automatisation de la notification aux citoyens. Le problème allemand existe donc également en Autriche.

Les rapports font état d'un fonctionnement technique stable et d'une marge d'erreur minimale. Le système informatique est conforme à la norme ISO 27.001 et aux normes de sécurité BSI (BSI IT-Grundschutz-Standards).

Il y a aussi un suivi parlementaire. La Cour des comptes autrichienne et la commission des Finances contrôlent l'efficacité et la proportionnalité. En 2021, le législateur autrichien a considéré que le système était achevé et suffisamment performant, mais sans automatisation supplémentaire ni *data mining*. Depuis la mise en place du système, le fisc autrichien a déjà récupéré plus d'un milliard d'euros d'impôts et réduit de 40 % la durée des enquêtes fiscales.

Le registre n'est toutefois pas un instrument de recherche en soi. Il fournit uniquement des informations sur la localisation des comptes, les étapes ultérieures

onderzoeksprocedures verlopen. De overheid heeft geen *realtime* inzicht in financiële stroom van burgers.

Deze beperking is bewust ingebouwd om constitutionele proportionaliteit te respecteren. Als dat systeem wordt nu vergeleken met het Belgische CAP-systeem, dan stelt men vast dat de beheerder de OeNB is in Oostenrijk. In België is het de Nationale Bank, maar wel onder het gezag van de FOD Financiën.

De gebruiker zijn in Oostenrijk fiscus, justitie en de meldingsinstantie voor witwassen (A-FIU). In België is dat vrij gelijkaardig. In ons land ligt de nadruk op de inhoud van de gegevens, terwijl Oostenrijk zich beperkt tot identificatiegegevens, d.w.z. identiteit, maar ook contracten en saldo. Data-analyse is in Oostenrijk verboden, in België zal het worden toegelaten. Profileren is in Oostenrijk verboden, hier zal het worden toegelaten. De toegang is enkel op aanvraag, in België zal geautomatiseerde raadpleging mogelijk zijn.

De kennisgeving is verplicht, hier is die niet voorzien. Het toezicht gebeurt door de onafhankelijke DSB, in België is er geen specifiek toezichtsmechanisme, ondanks het goede werk van de gegevensbeschermingsautoriteit. Deze vergelijking toont dat Oostenrijk een duidelijker scheiding hanteert tussen beheer, gebruik en controle.

België daarentegen concentreert alle functies binnen één administratieve hiërarchie. In Oostenrijk is elke beperking van het recht op gegevensbescherming grondwettelijk getoetst aan artikel 1 van de Privacywet en artikel 8 van het EVRM. In België is artikel 22 van de Grondwet van toepassing, maar er bestaat geen afzonderlijke constitutionele toets door het Grondwettelijk Hof voor de CAP-verwerking.

Het Belgische CAP is gekoppeld aan verschillende interne platformen van de FOD Financiën, dus door in de toekomst het *datamining* project *money control*. Hierdoor kan in België in de toekomst automatische risicoscores worden gegenereerd, iets wat in Oostenrijk grondwettelijk ondenkbaar is. In Oostenrijk is de menselijke tussenkomst verplicht bij elke beslissing tot onderzoek. In België kan *money control* algoritmisch beslissen welke dossiers over risico vormen, zonder individuele motiveren.

Het Oostenrijkse systeem garandeert dus de menselijke beoordeling, terwijl het Belgische model evolueert naar

se déroulant par le biais de procédures d'enquête classiques. Les autorités n'ont pas d'accès en temps réel aux flux financiers des citoyens.

Cette limitation a été délibérément mise en place afin de respecter la proportionnalité constitutionnelle. Si l'on compare ce système au système du PCC belge, on constate qu'en Autriche, le gestionnaire est l'OeNB. En Belgique, ce rôle est assuré par la Banque nationale, mais sous l'autorité du SPF Finances.

En Autriche, les utilisateurs sont le fisc, la justice et l'autorité de déclaration en matière de blanchiment (A-FIU). En Belgique, la situation est assez similaire. Dans notre pays, le contenu des données est plus étendu, tandis que l'Autriche se limite aux données d'identification, c'est-à-dire l'identité, mais aussi les contrats et le solde. L'analyse des données est interdite en Autriche, tandis qu'elle sera autorisée en Belgique. Le profilage est interdit en Autriche alors qu'il sera autorisé chez nous. L'accès n'est possible que sur demande, tandis que la Belgique permettra la consultation automatisée.

La notification est obligatoire, contrairement à la Belgique. La surveillance est assurée par l'organe indépendant, *Datenschutzbehörde* (DSB), tandis que la Belgique n'a pas prévu de mécanisme de surveillance spécifique, malgré l'excellent travail de l'Autorité de protection des données. Cette comparaison montre que l'Autriche scinde plus clairement la gestion, l'utilisation et le contrôle.

La Belgique, en revanche, concentre toutes les fonctions au sein d'une seule hiérarchie administrative. En Autriche, toute restriction du droit à la protection des données est contrôlée à la lumière de l'article 1^{er} de la législation relative à la protection de la vie privée et de l'article 8 de la CEDH. En Belgique, l'article 22 de la Constitution est d'application, mais le traitement dans le cadre du PCC n'est soumis à aucun contrôle de constitutionnalité distinct par la Cour constitutionnelle.

Le PCC belge est relié à différentes plateformes internes du SPF Finances. Dans le cadre du projet d'exploration de données *money control*, des scores de risque en Belgique pourront donc être générés automatiquement, ce qui est inconcevable du point de vue constitutionnel en Autriche puisque l'intervention humaine y est obligatoire pour toute décision d'enquête. À l'inverse, en Belgique, *money control* pourra décider algorithmiquement quels dossiers présentent un risque, sans justification individuelle.

Le système autrichien garantit dès lors une évaluation par une personne humaine tandis que le modèle

de facto geautomatiseerde selectie. In Oostenrijk is er ook een proportionaliteitsanalyse gedaan.

Volgens de Oostenrijkse rechtsleer moet elk financieel toezicht worden getoetst aan drie constitutionele criteria:

- dient het middel een legitiem doel?
- bestaat er een minder indringend intrusief alternatief?
- de noodzakelijkheid: is de privacy-inbreuk in verhouding tot het nagestreefde voordeel?

Het Oostenrijkse systeem voldoet aan deze drie voorwaarden. Het is geschikt, het gaat over een effectief opsprongen van fraude. Het is noodzakelijk, want er is geen lichter alternatief. En het is evenredig, want er is geen inhoudelijke data. Er is een menselijke tussenkomst en er is toezicht.

Het Belgische *money control* daarentegen voldoet enkel aan het eerste criterium. Zodra het algoritme screenen van burgers dat zou toelaten, schendt het de noodzakelijkheid en de evenredigheid, omdat algemeenanalyse nooit het minst ingrijpende middel kan zijn. De commissie beschouwt het Oostenrijkse model als een *best practice* binnen de implementatie van de Richtlijn 2019/1153.

In haar evaluatie van 2021 vermeldt de EU-commissie het volgende: Oostenrijkse centrale registratie, beheerd door de Nationale Bank, zorgt voor effectief toegang tot competente autoriteiten terwijl volledige toegang met de data-beveiligingsprincipes van de GDPR wordt beheerd. Ook de Europese toezichthouder voor gegevensbescherming, de EDPS, heeft het Oostenrijkse systeem positief beoordeeld, omdat het profilering uitsluit en menselijke controle verankert.

Hoewel het systeem in Oostenrijk wordt geprezen, zijn er toch enkele terugkerende discussies in de Oostenrijkse doctrine.

— Decentralisatie versus centralisatie

Duitsland is het gedecentraliseerd. Sommige juristen pleiten voor meer decentralisatie om de risico's van cyberaanvallen te beperken. Dat is een zeer legitieme opmerking.

belge évolue vers une sélection automatisée *de facto*. En Autriche, une analyse de la proportionnalité a également été menée.

Selon la doctrine juridique autrichienne, il convient de vérifier si la surveillance financière respecte trois critères constitutionnels:

- le moyen poursuit-il un objectif légitime?
- existe-t-il une alternative moins intrusive?
- la nécessité: l'atteinte à la vie privée est-elle proportionnée à l'avantage recherché?

Le système autrichien remplit ces trois conditions. Il est adéquat, car il vise effectivement à détecter les cas de fraude. Il est nécessaire, car il n'existe pas d'alternative moins contraignante. Et il est proportionné, car il ne vise pas de données de fond. Il est assorti d'une intervention humaine et d'un contrôle.

Le *money control belge* ne remplit en revanche que le premier critère. Dès lors que l'algorithme permet de profiler les citoyens, il enfreint les principes de nécessité et de proportionnalité, car l'analyse générale ne pourra jamais être le moyen le moins intrusif. La Commission considère que le modèle autrichien est une bonne pratique dans le cadre de la mise en œuvre de la directive 2019/1153.

Dans son évaluation de 2021, la Commission européenne indique en effet que le registre central autrichien, géré par la Banque nationale, garantit un accès efficace aux autorités compétentes, mais l'accès complet est soumis aux principes de sécurité des données du RGPD. Le Contrôleur européen de la protection des données (CEPD) a également évalué positivement le système autrichien, parce qu'il exclut le profilage et consacre le contrôle humain.

Bien que l'on vante les mérites du système autrichien, certaines questions sont récurrentes dans la doctrine autrichienne.

— Décentralisation versus centralisation

Le système allemand se caractérise par sa décentralisation. Certains juristes préconisent une décentralisation accrue afin de limiter les risques de cyberattaques. Il s'agit d'une recommandation tout à fait légitime.

— *De tijdige kennisgeving*

Hetzelfde probleem als in Duitsland: ook in Oostenrijk stelt men vast dat de kennisgeving niet altijd sterk toepast, en dat uitzonderingen wegens onderzoeksbelangen soms zeer ruim worden geïnterpreteerd.

— *De beperkte burgerbekendheid*

Niet veel burgers weten dat ze het recht hebben op inzagen. En daarom overweegt een publiekportaal, een beetje geïnspireerd door het Belgische *MyData* systeem.

Toch verandert deze kritiek weinig aan de juridische kern. Het Oostenrijkse model blijft strikt transparant en grondwettelijk robuust.

Uit het Oostenrijkse voorbeeld kunnen voor België de volgende belangrijke lessen worden getrokken:

— de institutionele scheiding: de beheerder van de gegevens mag niet dezelfde zijn als de gebruiker ervan;

— de formele legaliteit: elke bevoegdheid moet in de wet worden opgenomen en niet in uitvoeringsbesluiten;

— het beperkingsprincipe: enkel identificatiegegevens en geen gedragsgegevens;

— het verbod op datamining: automatische analyses of profilering zijn niet toegestaan;

— de rechtsbescherming: kennisgeving, inzage, klacht en toezicht.

Om hetzelfde niveau van rechtsstatelijke bescherming te bereiken als in Oostenrijk ware het aangewezen dat België het systeem zou onderbrengen bij een onafhankelijke instelling. Profilering en datamining dienen wettelijk te worden uitgesloten, wat in België volgens hem nu niet het geval is aangezien de wetgeving dat momenteel toelaat. De kennisgevingsplicht dient te worden ingevoerd en het gebruik moet worden beperkt tot individuele, gemotiveerde onderzoeken.

De heer Van Quickenborne waarschuwt dat België zonder deze hervormingen, met het project *money control*, een uniek precedent in Europa dreigt te scheppen: een fiscale administratie die algoritmische toegang heeft tot bankgegevens van alle burgers, zonder voorafgaande

— *Notification dans les délais impartis*

Le problème est le même qu'en Allemagne: force est de constater qu'en Autriche également, la notification n'est pas toujours appliquée strictement, et que la notion d'exception pour les intérêts de l'enquête est parfois interprétée très largement.

— *Connaissance limitée du système dans le chef des citoyens*

Peu de citoyens savent qu'ils ont le droit de consulter leurs données. C'est pourquoi les autorités envisagent de créer un portail public, inspiré en partie du système belge *MyData*.

Ces critiques n'ébranlent toutefois guère l'ossature juridique du modèle autrichien, qui demeure parfaitement transparent et constitutionnellement solide.

La Belgique peut tirer les enseignements importants suivants de l'exemple autrichien:

— séparation institutionnelle: le gestionnaire des données ne peut pas en être l'utilisateur;

— légalité formelle: chaque compétence doit être inscrite dans la loi, et pas dans des arrêtés d'exécution;

— principe de restriction: seules sont autorisées les données d'identification, et pas les données comportementales;

— interdiction de l'exploration de données: les analyses et le profilage automatiques ne sont pas autorisés;

— protection des droits: notification, consultation, plainte et surveillance.

Pour garantir le même degré de protection de l'état de droit qu'en Autriche, il aurait été indiqué que la Belgique confie la gestion du système visé à un organe indépendant. Par ailleurs, la loi devrait interdire le profilage et l'exploration de données, ce qui, selon l'intervenant, n'est aujourd'hui pas le cas dans notre pays dès lors qu'ils y sont légalement autorisés. De plus, il faudrait instaurer l'obligation de notification et restreindre l'usage de ces techniques aux enquêtes individuelles et motivées.

M. Van Quickenborne avertit qu'avec son projet *money control*, et en l'absence de ces réformes, la Belgique risque de créer un précédent unique en Europe, à savoir autoriser une administration fiscale à accéder via des algorithmes aux données bancaires de l'ensemble des

motivering of wenselijke toetsing. Geen enkel ander EU-land, ook Oostenrijk niet, is ooit zo ver gegaan.

Hij besluit dat het Oostenrijkse *Kontenregistergesetz* een toonbeeld vormt van rechtsstatelijke terughoudendheid in tijden van digitalisering. Het bewijst dat technologische efficiëntie niet hoeft te botsen met grondrechtelijke bescherming. Door de functies te scheiden, het toezicht te institutionaliseren en datamining uit te sluiten, heeft Oostenrijk een model gecreëerd dat transparantie combineert met vertrouwen.

Het Oostenrijkse systeem staat symbool voor een fundamenteel principe: financiële transparantie mag niet leiden tot algoritmische controle. België zou er volgens hem dan ook goed aan doen om dit principe te omarmen alvorens het project *money control* verder uit te rollen. Wat in Oostenrijk grondwettelijk verboden is, kan volgens hem in België nooit vanzelfsprekend legaal worden zonder een herziening van artikel 22 van de Grondwet en een uitdrukkelijke wetgevende toets. Het Oostenrijkse model toont aan dat de grens tussen de fiscale controle en de digitale surveillance niet technologisch, maar constitutioneel is. Enkel een staat die zichzelf grenzen oplegt, kan daadwerkelijk de vrijheid van zijn burgers beschermen.

Hij komt vervolgens tot het model van Nederland.

De heer Van Quickenborne stelt vast dat in Nederland in de afgelopen decennia heel wat is gebeurd, onder meer de bekende toeslagenaffaire. Nederland heeft in de voorbije dertig jaar een complex maar zorgvuldig uitgebalanceerd systeem ontwikkeld voor de verwerking en de uitwisseling van financiële gegevens ten behoeve van fiscale, financiële en antiwitwasdoeleinden. Hoewel Nederland geen centraal bankregister heeft zoals Duitsland of Oostenrijk, beschikt het over een gedistribueerd stelsel van informatieverplichtingen waarin financiële instellingen, toezichthouders en overheidsdiensten juridisch verplicht samenwerken.

Het Nederlandse model wordt gekenmerkt door de volgende drie principes:

— legaliteit: elke gegevensverwerking moet expliciet in de wet zijn verankerd;

— proportionaliteit: de gegevensverwerking mag niet verder gaan dan noodzakelijk is voor het beoogde doel;

citoyens, sans devoir fournir de motivation préalable ni être soumis à des contrôles souhaitables. Aucun autre pays européen, pas même l'Autriche, n'est allé aussi loin.

L'intervenant conclut en indiquant que la loi autrichienne sur le registre des comptes bancaires constitue un modèle de retenue à l'égard de l'état de droit en ces temps de numérisation. Elle prouve que l'efficacité technologique ne doit pas forcément entrer en conflit avec la protection constitutionnelle. En séparant les fonctions, en institutionnalisant la surveillance et en excluant l'exploration de données, l'Autriche a créé un modèle conjuguant transparence et confiance.

Le système autrichien symbolise un principe fondamental: la transparence financière ne peut pas déboucher sur un contrôle algorithmique. Selon l'intervenant, la Belgique serait donc bien inspirée de souscrire à ce principe avant de poursuivre la mise en œuvre du projet *money control*. Le membre estime que ce qui est interdit par la Constitution en Autriche ne peut évidemment pas être autorisé par la loi en Belgique sans une révision de l'article 22 de la Constitution et un examen législatif explicite. Le modèle autrichien montre que la frontière entre le contrôle fiscal et la surveillance numérique est de nature non pas technologique mais constitutionnelle. Seul un État qui se fixe des limites peut réellement protéger la liberté de ses citoyens.

L'intervenant en arrive ensuite au modèle néerlandais.

M. Van Quickenborne constate que beaucoup d'événements se sont produits aux Pays-Bas ces dernières décennies, notamment le fameux scandale des allocations familiales. Ces trente dernières années, les Pays-Bas ont mis au point un système complexe mais soigneusement équilibré pour le traitement et l'échange de données financières à des fins fiscales, financières et de lutte contre le blanchiment d'argent. Bien que les Pays-Bas ne disposent pas d'un registre bancaire central comme l'Allemagne ou l'Autriche, ils ont mis en place un système réparti d'obligations d'information dans le cadre duquel les institutions financières, les autorités de surveillance et les services publics sont légalement tenus de coopérer.

Le modèle néerlandais se fonde sur les trois principes suivants:

— légalité: tout traitement de données doit reposer sur un fondement légal explicite;

— proportionnalité: le traitement des données ne doit pas aller au-delà de ce qui est nécessaire pour atteindre l'objectif visé;

— menselijke toetsing: een automatische besluitvorming zonder menselijke tussenkomst is principieel verboden.

In tegenstelling tot de uitbreiding van *money control* is de Nederlandse benadering niet gebaseerd op centralisatie of datamining, maar op casusgebonden informatie-uitwisseling. Het systeem laat rechtstreekse bevestigingen toe die gekoppeld zijn aan concrete fiscale of strafrechtelijke onderzoeken.

De Nederlandse belastingadministratie was tot eind jaren negentig grotendeels afhankelijk van papieren informatieverplichtingen en van de vrijwillige medewerking van banken. De Belastingdienst kon gegevens opvragen op grond van artikel 47 van de Algemene wet inzake rijksbelastingen (AWR), dat elke burger en instelling verplicht om gegevens te verstrekken die voor de belastingheffing van belang kunnen zijn. De banksector genoot destijds echter een feitelijk bankgeheim, beschermd door de civielrechtelijke vertrouwensplicht in artikel 7:457 van het Burgerlijk Wetboek. Slechts in uitzonderlijke gevallen kon de fiscus via de rechter-commissaris toegang krijgen tot rekeninginformatie. Vanaf 2001 voerde Nederland onder druk van internationale afspraken van de OESO, de EU en de GAFI een reeks hervormingen door.

Er kwamen twee wetten: de Wet identificatie bij dienstverlening (WID) en de Wet melding ongebruikelijke transacties (MOT), voorlopers van de latere WWFT (Wet ter voorkoming van witwassen en financieren van terrorisme). De Belastingdienst kreeg bovendien de bevoegdheid om elektronische gegevensuitwisseling te eisen, onder meer via de Verzamelwet Systeem Financiën 2001 en de oprichting van de FIOD (Fiscale inlichtingen- en opsporingsdienst) als gespecialiseerde eenheid. Vanaf 2005 werden banken verplicht om bij te dragen aan automatische gegevenslevering, bijvoorbeeld inzake rente, dividenden en spaartegoeden.

Ook de Europese regelgeving heeft een aanzienlijke invloed gehad, met name de vierde en vijfde Europese antiwitwasrichtlijn en de invoering van de *Common Reporting Standard* (CRS) door de OESO, wat tot verdere internationale integratie heeft geleid. Nederland trad toe tot het internationale uitwisselingsnetwerk voor

— contrôle humain: toute prise de décision automatisée sans intervention humaine est en principe interdite.

Contrairement à l'extension de *money control*, l'approche néerlandaise n'est pas basée sur la centralisation ou l'exploration de données, mais sur l'échange d'informations au cas par cas. Ce système autorise les requêtes directes liées à des enquêtes fiscales ou pénales concrètes.

Jusqu'à la fin des années 1990, l'administration fiscale néerlandaise dépendait en grande partie du respect d'obligations imposant de fournir des informations sur papier et de la coopération volontaire des banques. L'administration fiscale néerlandaise pouvait demander des informations en vertu de l'article 47 de la loi néerlandaise générale sur les impôts (*Algemene wet inzake rijksbelastingen* (AWR)), qui obligeait chaque citoyen et chaque institution à fournir toute information susceptible d'être digne d'intérêt dans le cadre de l'imposition. À l'époque, le secteur bancaire bénéficiait toutefois dans les faits d'un secret bancaire, protégé par l'obligation de confidentialité prévue à l'article 7:457 du Code civil néerlandais. Ce n'est que dans des cas exceptionnels que le fisc pouvait accéder aux informations bancaires, par l'intermédiaire du juge-commissaire. À partir de 2001, sous la pression des accords internationaux conclus au sein de l'OCDE, de l'Union européenne et du GAFI, les Pays-Bas ont mis en œuvre une série de réformes.

Deux lois ont ainsi vu le jour: la loi relative à l'identification lors de la prestation de services (*Wet identificatie bij dienstverlening* – WID) et la loi relative à la notification des transactions inhabituelles (*Wet melding ongebruikelijke transacties* – MOT), qui ont ouvert la voie à l'adoption de la loi sur la prévention du blanchiment d'argent et du financement du terrorisme (*Wet ter voorkoming Van witwassen en financieren Van terrorisme* – WWFT). L'administration fiscale a également été habilitée à exiger l'échange électronique de données, notamment par le biais de la loi fourre-tout "*Systeem Financiën 2001*" et de la création d'une unité spécialisée, le Service de l'information et de la recherche en matière de fiscalité (*Fiscale inlichtingen- en opsporingsdienst* – FIOD). Depuis 2005, les banques sont tenues de contribuer à la transmission automatique de données relatives notamment aux intérêts, aux dividendes et aux avoirs d'épargne.

La réglementation européenne a également eu une influence considérable – notamment à travers les quatrième et cinquième directives anti-blanchiment –, tout comme la norme commune de déclaration (NCD) introduite par l'OCDE. Cela a permis une intégration internationale accrue. Les Pays-Bas ont ainsi adhéré au réseau

fiscale informatie (*automatic exchange of information*), waardoor jaarlijks gegevens over buitenlandse rekeningen automatisch worden uitgewisseld tussen belastingdiensten. In 2018 werd de WWFT volledig herschreven. Deze wet legt aan banken, notarissen, accountants en advocaten een meldingsplicht op voor verdachte transacties, die moeten worden gerapporteerd aan de Financiële Inlichtingeneenheid (FIU) in Nederland. Sinds 2020 beschikt Nederland bovendien over een UBO-register (*Ultimate Beneficial Owners*), dat de aandeelhoudersstructuren van vennootschappen openbaar maakt. Dit register wordt beheerd door de Kamer van Koophandel en is eveneens een Europese verplichting. Nederland beschikt aldus over een zeer gedifferentieerd stelsel waarin financiële gegevens via verschillende kanalen toegankelijk zijn, zonder één gecentraliseerde databank.

De Nederlandse Algemene Wet inzake Rijksbelastingen (AWR) vormt de ruggengraat van de fiscale informatiebevoegdheden. Artikel 47 van voormelde wet bepaalt dat iedereen verplicht is desgevraagd gegevens te verstrekken aan de inspecteur, voor zover die relevant zijn voor de belastingheffing. Banken vallen onder deze verplichting, mits het verzoek van de inspecteur concreet gemotiveerd en proportioneel is. Het verzoek moet betrekking hebben op een geïdentificeerde belastingplichtige, noodzakelijk zijn voor de belastingheffing en berusten op een wettelijke grondslag. De Hoge Raad heeft, onder meer in de arresten van 23 juni 1993 en 20 maart 2015, bevestigd dat deze bevoegdheid geen onbeperkt inzagerecht verleent. De inspecteur mag niet “vissend” opvragen; banken moeten enkel die gegevens verstrekken die relevant zijn voor het specifieke dossier.

Voormelde WWFT vormt de tweede pijler van het systeem. Deze wet voert de Europese antiwitwasrichtlijnen uit en verplicht banken tot cliëntenidentificatie (*Know Your Customer* – KYC), risicobeoordeling en melding van ongebruikelijke transacties bij de FIU Nederland. De FIU (*Financial Intelligence Unit*), gevestigd in Driebergen, maakt deel uit van de politie, maar functioneert als een onafhankelijke meldinstantie. Zij ontvangt meldingen, analyseert die en kan verdachte transacties doorgeven aan de opsporingsautoriteiten. De WWFT verplicht banken tevens tot het bijhouden van rekening- en transactiegegevens, maar enkel voor interne risicobeheersing en wettelijke meldplichten, niet voor de centrale opslag bij de overheid.

De Wet op het financieel toezicht (WFT) vormt de derde pijler. Deze wet regelt het prudentiële en integriteitstoezicht

international d'échange automatique d'informations fiscales (*automatic exchange of information*), dans le cadre duquel des données relatives à des comptes étrangers sont chaque année échangées automatiquement entre les administrations fiscales. La WWFT a été entièrement révisée en 2018. Elle impose aux banques, aux notaires, aux experts-comptables et aux avocats l'obligation de déclarer les opérations suspectes à la Cellule de renseignement financier (*Financiële Inlichtingeneenheid* – FIU) des Pays-Bas. Depuis 2020, le pays dispose également d'un registre UBO (*Ultimate Beneficial Owners*), qui publie les structures d'actionnariat des sociétés. Ce registre, géré par la Chambre de commerce, résulte aussi d'une obligation européenne. Les Pays-Bas disposent ainsi d'un système très différencié, dans lequel les informations financières sont accessibles par divers canaux, sans banque de données centralisée.

La loi générale néerlandaise relative aux impôts d'État (*Algemene Wet inzake Rijksbelastingen* – AWR) constitue le fondement des compétences en matière d'informations fiscales. L'article 47 de cette loi prévoit que toute personne est tenue de fournir les informations réclamées par l'inspecteur, dans la mesure où elles présentent un intérêt pour l'imposition. Les banques sont également soumises à cette obligation, à condition que la demande de l'inspecteur soit concrètement motivée et proportionnée. La demande doit concerner un contribuable identifié, être nécessaire à l'imposition et reposer sur une base légale. La Cour suprême des Pays-Bas a confirmé, notamment dans ses arrêts des 23 juin 1993 et 20 mars 2015, que cette compétence ne confère pas un droit d'accès illimité. L'administration ne peut pas effectuer de demandes aléatoires: les banques sont uniquement tenues de fournir les informations pertinentes pour le dossier concerné.

La WWFT précitée constitue le deuxième pilier du dispositif. Cette loi transpose les directives européennes en matière de lutte contre le blanchiment d'argent et impose aux banques l'identification de leurs clients (*Know Your Customer* – KYC), l'évaluation des risques ainsi que la notification des transactions inhabituelles auprès de la FIU (*Financial Intelligence Unit*) des Pays-Bas. La FIU, établie à Driebergen, fait partie de la police, mais fonctionne comme un organe de notification indépendant. Elle reçoit et analyse les notifications, et peut transmettre les transactions suspectes aux services d'enquête. La WWFT oblige également les banques à conserver les informations relatives aux comptes et aux transactions, mais uniquement aux fins de leur gestion interne des risques et du respect de leurs obligations légales de notification, et non pour un stockage centralisé par l'État.

La loi sur la supervision financière (*Wet op het financieel toezicht* – WFT) constitue le troisième pilier du

op banken, verzekeraars en beleggingsinstellingen. De Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten (AFM) zijn in Nederland de belangrijkste toezichthouders. Hoewel de WFT geen directe fiscale toepassing heeft, speelt zij wel een rol in de informatie-uitwisseling met de Belastingdienst en de FIU. Mits dit noodzakelijk is voor de vervulling van een wettelijke taak kan de DNB op grond van artikel 1:89 van de WFT informatie delen met de belastingdienst. Deze bepaling vormt de juridische brug tussen financieel toezicht en fiscale handhaving, maar blijft beperkt tot strikt individuele gevallen.

De vierde pijler van de Nederlandse wetgeving is de Algemene Verordening Gegevensbescherming (AVG/GDPR). De AVG is rechtstreeks van toepassing in Nederland en de kernbeginselen ervan – rechtmatigheid, doelbinding, dataminimalisatie, transparantie en menselijke toetsing – gelden volledig voor overheidsverwerking. Artikel 22 van de AVG verbiedt geautomatiseerde besluitvorming zonder menselijke tussenkomst. Nederland heeft dit beginsel versterkt via de Uitvoeringswet AVG. Overeenkomstig artikel 40 van voormelde wet mag de overheid automatische besluitvorming alleen toepassen indien de wet dit expliciet toestaat en er adequate waarborgen bestaan. Na de toeslagenaffaire in 2020 heeft de Tweede Kamer dit principe nogmaals bevestigd. Risicoselectie zonder menselijke beoordeling wordt als onrechtmatig beschouwd.

Over de bevoegde instellingen in Nederland en de rol die zij vervullen. De Belastingdienst is verantwoordelijk voor de uitvoering van de belastingwetten maar beschikt niet over een permanent financieel register. Informatie over bankrekeningen wordt verkregen via vrijwillige opgave door burgers, gerichte verzoeken aan banken op grond van artikel 47 van de AWR, of internationale gegevensuitwisseling via CRS en FATCA. De Belastingdienst gebruikt deze gegevens uitsluitend voor belastingheffing en toezicht. De interne directie toezicht en handhaving van de Belastingdienst voert, uitsluitend op fiscale gegevens en niet op bankdata, risicoanalyses uit.

Naast de Belastingdienst is er de FIOD (Fiscale inlichtingen- en opsporingsdienst), een opsporingsdienst van het ministerie van Financiën met bijzondere bevoegdheden. De FIOD onderzoekt fraude, witwassen en corruptie en kan financiële gegevens opvragen in het kader van strafrechtelijke onderzoeken. Zij werkt samen

dispositief. Cette loi encadre le contrôle prudentiel ainsi que le contrôle de l'intégrité des banques, des assureurs et des organismes de placement collectif. La Banque des Pays-Bas (*De Nederlandsche Bank* – DNB) et l'Autorité des marchés financiers (*Autoriteit Financiële Markten* – AFM) sont les principaux organes de supervision du pays. Bien que la WFT ne produise aucun effet fiscal direct, elle joue un rôle dans les échanges d'informations avec l'administration fiscale et la FIU. Lorsque cela est nécessaire à l'accomplissement d'une mission légale, la DNB peut, en vertu de l'article 1:89 de la WFT, transmettre des informations à l'administration fiscale. Cette disposition établit l'articulation entre la supervision financière et le contrôle fiscal, tout en restant limitée à des cas strictement individuels.

Le quatrième pilier de la législation néerlandaise est le Règlement général sur la protection des données (RGPD). Le RGPD, applicable directement aux Pays-Bas, impose ses principes fondamentaux – licéité, finalité, minimisation des données, transparence et contrôle humain – au traitement des données par les autorités publiques. L'article 22 du RGPD interdit la prise de décision automatisée sans intervention humaine. Les Pays-Bas ont renforcé ce principe par la loi d'exécution du RGPD. Conformément à l'article 40 de cette loi, l'administration ne peut recourir à une décision automatisée que si la loi l'autorise explicitement et si des garanties adéquates sont prévues. À la suite de l'affaire des allocations familiales en 2020, la deuxième chambre a réaffirmé ce principe: toute sélection des risques effectuée sans évaluation humaine est considérée comme illégale.

L'intervenant évoque les institutions compétentes aux Pays-Bas et le rôle qu'elles exercent. L'administration fiscale est responsable de l'application des lois fiscales, mais elle ne dispose pas d'un registre financier permanent. Les informations relatives aux comptes bancaires sont obtenues au moyen de communications volontaires par les citoyens, de demandes adressées aux banques en vertu de l'article 47 de la loi générale sur les impôts nationaux (AWR), ou de l'échange international de données en vertu des réglementations CRS et FATCA. L'administration fiscale n'utilise ces données qu'aux fins de la taxation et du contrôle. La direction interne chargée du contrôle et de l'application de la loi au sein de l'administration fiscale réalise des analyses de risques qui reposent exclusivement sur des données fiscales et non sur des données bancaires.

Outre l'administration fiscale, il existe aux Pays-Bas un service de renseignements et d'enquête en matière fiscale, dénommé FIOD, qui dépend du ministère des Finances et qui a des compétences particulières. Le FIOD enquête sur les cas de fraude, de blanchiment et de corruption, et peut réclamer des données financières

met de FIU en de politie onder toezicht van het openbaar ministerie en kan via artikel 126 van het Wetboek van Strafvordering gegevensvorderingen doen bij banken, mits goedkeuring van een officier van justitie, wat extra rechtsbescherming biedt.

De derde instelling is de FIU (*Financial Intelligence Unit*), vergelijkbaar met de Belgische CFI. De FIU ontvangt jaarlijks meer dan 1,2 miljoen meldingen van ongebruikelijke transacties van banken, notarissen, accountants en makelaars. Hiervan worden ongeveer 80.000 meldingen na analyse als verdacht aangemerkt. De FIU koppelt deze gegevens niet aan fiscale gegevensbanken; de verwerking gebeurt uitsluitend binnen het kader van de WWFT en enkel voor criminaliteitsbestrijding.

De vierde instelling is de Nederlandsche Bank (DNB), toezichthouder op financiële instellingen en beheerder van risicodata, zonder bevoegdheid om individuele klantinformatie te raadplegen of te delen met de fiscus. De DNB houdt uitsluitend prudentiële informatie bij, zoals solvabiliteit, liquiditeit en integriteit van de banken.

Daarnaast wijst het lid op de Autoriteit Persoonsgegevens (AP), de onafhankelijke toezichthouder op de naleving van de AVG. De AP beschikt over onderzoeks-, advies- en sanctiebevoegdheden. Na de toeslagenaffaire kreeg de Belastingdienst in 2021 een boete van 3,7 miljoen euro opgelegd. De AP heeft ook gewaarschuwd tegen het gebruik van algoritmen en risicoprofielen in een fiscale context zonder expliciete wettelijke basis.

De heer Van Quickenborne vestigt de aandacht van de leden erop dat Nederland niet werkt met één centrale databank maar met gescheiden registers die samen een federatief systeem vormen. Bankgegevens blijven bij de banken en zijn raadpleegbaar via artikel 47 van de AWR of strafrechtelijke verordeningen. Transactiegegevens worden gemeld aan de FIU bij verdenking, het UBO-register is openbaar voor bevoegde instanties en buitenlandse rekeningen worden verwerkt via CRS en FATCA. De fiscale kerngegevens blijven bij de Belastingdienst. Deze gedeelde, niet-gecentraliseerde architectuur voorkomt marktconcentratie en beperkt het risico van massale dataverwerking.

dans le cadre d'enquêtes pénales. Il collabore avec la *Financial Intelligence Unit* (FIU) et avec la police sous la supervision du ministère public, et peut requérir des données auprès des banques conformément à l'article 126 du Code de procédure pénale, moyennant l'accord d'un procureur du Roi, qui offre une protection juridique supplémentaire.

La troisième institution, la FIU (*Financial Intelligence Unit*), est comparable à la CTIF belge. La FIU reçoit chaque année plus de 1,2 million de signalements de transactions inhabituelles de la part de banques, de notaires, de comptables et de courtiers. Après analyse, environ 80.000 de ces signalements sont jugés suspects. La FIU ne relie pas ces données aux banques de données fiscales; le traitement est réalisé exclusivement dans le cadre de la WWFT et uniquement à des fins de lutte contre la criminalité.

La quatrième institution est la Banque des Pays-Bas (DNB), qui est l'autorité de surveillance des institutions financières et le gestionnaire des données concernant les risques, et qui n'est pas habilitée à consulter les informations individuelles des clients, ni à les partager avec l'administration fiscale. La DNB ne conserve que des informations prudentielles concernant, par exemple, la solvabilité, la liquidité et l'intégrité des banques.

L'intervenant mentionne aussi l'autorité chargée des données à caractère personnel (*Autoriteit Persoonsgegevens*, AP), qui est le contrôleur indépendant du respect du RGPD. L'AP dispose de compétences d'enquête, d'avis et de sanction. À la suite de l'affaire des allocations, une amende de 3,7 millions d'euros a été infligée à l'administration fiscale en 2021. L'AP a aussi mis en garde contre l'utilisation d'algorithmes et de profils de risques dans un contexte fiscal, sans base légale explicite.

M. Van Quickenborne attire l'attention des membres sur le fait que les services des Pays-Bas n'utilisent pas une banque de données centrale unique, mais plusieurs registres séparés qui forment ensemble un système fédéré. Les données bancaires sont conservées par les banques et peuvent être consultées en vertu de l'article 47 de la loi générale sur les impôts nationaux (AWR) ou d'ordonnances pénales. Les données relatives aux transactions sont signalées à la FIU en cas de suspicion de fraude, le registre UBO est public pour les instances compétentes, et les comptes étrangers sont traités en vertu des réglementations CRS et FATCA. Les données fiscales essentielles sont conservées par l'administration fiscale. Cette architecture partagée et décentralisée évite une concentration de ce marché et limite le risque de traitement massif de données.

Nederland heeft aldus een systeem dat is gebouwd op *checks and balances*:

— legaliteit: alle gegevensverwerkingen moeten berusten op expliciete wettelijke bepalingen. Er bestaat geen open mandaat voor de gegevensverwerking;

— transparantie: de overheid is verplicht om burgers te informeren over gegevensverwerking (artikelen 13 en 14 van de AVG), met uitzondering van lopende strafrechtelijke onderzoeken;

— onafhankelijk toezicht: de AP oefent toezicht uit op alle betrokken overheden; daarnaast houden de Tweede Kamer, de Algemene Rekenkamer en de Nationale Ombudsman toezicht en signaleren misbruik. De parlementaire enquête naar de toeslagen van 2021 heeft de gevoeligheid voor waarborgen nog verder vergroot.

De heer Van Quickenborne bespreekt vervolgens de automatisering en benadrukt dat artikel 40 van de Uitvoeringswet AVG en artikel 22 van de AVG automatische beslissingen zonder menselijke tussenkomst verbieden. Na 2020 heeft het kabinet expliciet bepaald dat alle risicoselecties door mensen moeten worden gevalideerd, waardoor geautomatiseerde *money control*-achtige mechanismen worden uitgesloten.

Wat de constitutionele en Europese inbedding betreft, verwijst het lid naar artikel 10 van de Nederlandse Grondwet dat het recht op eerbiediging van de persoonlijke levenssfeer inhoudt. De jurisprudentie van de Raad van State van Nederland bevestigt dat elke inmenging op de privacy een wettelijke en proportionaliteitstoets vereist. Artikel 8 van het EVRM beschermt dit recht binnen de Europese context. Nederland past consequent de jurisprudentie van het Europees Hof van Justitie strikt toe, met name de arresten *Digital Rights Ireland* (C-293/12), *Tele2 Sverige* (C-203/15) en *La Quadrature du Net* (C-511/18). Wat de Nederlandse jurisprudentie betreft, herinnert hij de leden eraan dat in 2020 de rechtbank van Den Haag heeft geoordeeld dat de wetgeving die de inzet van het Systeem Risico Indicatie (SyRI; een systeem dat risicoprofielen genereert met gegevens uit sociale zekerheid en belastingen) regelt in strijd is met het hoger recht. De wetgeving voldoet volgens de rechtbank niet aan artikel 8 van het Europees Verdrag voor de Rechten voor de Mens (EVRM). Sindsdien bestaat er in Nederland een juridisch en politiek taboe op algoritmische profilering door de overheid.

Les Pays-Bas disposent ainsi d'un système qui prévoit des contrôles et des contrepoids:

— légalité: tous les traitements de données doivent s'appuyer sur des dispositions légales explicites et aucun mandat ouvert n'a été prévu pour le traitement de données;

— transparence: les autorités publiques sont obligées d'informer les citoyens du traitement de données (articles 13 et 14 du RGPD), sauf dans le cadre d'enquêtes pénales en cours;

— contrôle indépendant: l'AP contrôle toutes les autorités publiques concernées. Par ailleurs, la Chambre basse (*Tweede Kamer*), la Cour des comptes des Pays-Bas (*Algemene Rekenkamer*) et le Médiateur national (*Nationale Ombudsman*) exercent un contrôle et signalent les abus. L'enquête parlementaire sur les allocations familiales de 2021 a encore accru la sensibilité aux garanties.

M. Van Quickenborne aborde ensuite la question de l'automatisation et souligne que l'article 40 de la loi d'application du RGPD et l'article 22 du RGPD interdisent les décisions automatisées sans intervention humaine. Après 2020, le cabinet a explicitement stipulé que toutes les sélections de risques doivent être validées par des personnes, ce qui exclut les mécanismes automatisés de type *money control*.

En ce qui concerne l'ancrage constitutionnel et européen, le membre renvoie à l'article 10 de la Constitution néerlandaise, qui garantit le droit au respect de la vie privée. La jurisprudence du Conseil d'État des Pays-Bas confirme que toute ingérence dans la vie privée doit être soumise à un contrôle de légalité et de proportionnalité. L'article 8 de la CEDH protège ce droit dans le contexte européen. Les Pays-Bas appliquent de manière cohérente et stricte la jurisprudence de la Cour de justice de l'Union européenne, en particulier les arrêts *Digital Rights Ireland* (C-293/12), *Tele2 Sverige* (C-203/15) et *La Quadrature du Net* (C-511/18). En ce qui concerne la jurisprudence néerlandaise, l'intervenant rappelle aux membres qu'en 2020, le tribunal de La Haye a jugé que la législation régissant l'utilisation du *Systeem Risico Indicatie* (SyRI; un système qui génère des profils de risque à partir de données provenant de la sécurité sociale et des impôts) était contraire au droit supérieur. Selon le tribunal, cette législation n'est pas conforme à l'article 8 de la Convention européenne des droits de l'homme (CEDH). Depuis lors, le profilage algorithmique par les pouvoirs publics est un sujet tabou sur le plan juridique et politique aux Pays-Bas.

De heer Van Quickenborne merkt op dat het Nederlandse systeem zich onderscheidt door de afwezigheid van centralisatie, het primaat van de wet, de menselijke toetsing en toezicht, de strikte doelbinding en een sterke constitutionele bescherming. Waar in België gegevens voor *data mining* zullen worden ingezet, beschouwt Nederland dit juridisch en ethisch als ontoelaatbaar. De fiscale administratie handelt in Nederland strikt binnen de wettelijke bevoegdheden en niet als data-analist. De praktijk in Nederland toont aan dat fiscale efficiëntie perfect kan samengaan met grondrechtelijke discipline. Het Nederlandse model vormt daardoor een voorbeeld van terughoudende moderniteit, waarin technologische innovatie nooit het principe van legaliteit doorbreekt.

De heer Van Quickenborne (Open Vld) vervolgt zijn vergelijking tussen het in Nederland van kracht zijnde systeem en de regeling die door het voorliggende wetsontwerp wordt voorgesteld. Hij gaat in op de respectieve implementatie ervan.

Concreet is dit de procedure in Nederland:

1. de inspecteur begint met het formuleren van een gemotiveerd verzoek;
2. de betrokken instantie, bijvoorbeeld een bank, beoordeelt of het verzoek in overeenstemming is met het wettelijk raamwerk;
3. bij twijfel kan de instantie de inspecteur vragen de reikwijdte van het verzoek te verduidelijken;
4. de gegevens worden verzonden via beveiligde digitale kanalen.

Het lid wijst erop dat de fiscus in Nederland niet het recht heeft blindelings onderzoeken te voeren; elk verzoek moet gebaseerd zijn op een specifieke grond, zoals een onregelmatigheid in een aangifte of een melding van de toezichtseenheid voor financiële verrichtingen (Financial Intelligence Unit, FIU). Die kwestie valt onder de regels van evenredigheid en subsidiariteit.

Wat de informatiestroom betreft, speelt Nederland een actieve rol in de automatische uitwisseling van financiële gegevens op internationaal vlak. Op grond van bepaalde overeenkomsten (CRS, FATC enzovoort) ontvangt de Nederlandse fiscus elk jaar een enorme hoeveelheid financiële informatie. Die informatie moet worden verwerkt in een gesloten en beveiligde omgeving, onder toezicht van een ambtenaar-functionaris voor gegevensbescherming – de tegenhanger van de

M. Van Quickenborne fait observer que le système néerlandais se distingue par l'absence de centralisation, la primauté de la loi, le contrôle et la surveillance humains, la limitation stricte de la finalité et une forte protection constitutionnelle. Alors qu'en Belgique, des données seront utilisées à des fins de *data mining*, les Pays-Bas considèrent cette pratique comme juridiquement et éthiquement inacceptable. Aux Pays-Bas, l'administration fiscale agit strictement dans le cadre de ses compétences légales et non en tant qu'analyste de données. La pratique aux Pays-Bas montre que l'efficacité fiscale est parfaitement compatible avec le respect des droits fondamentaux. Le modèle néerlandais constitue ainsi un exemple de modernité modérée, où l'innovation technologique ne transgresse jamais le principe de légalité.

M. Van Quickenborne (Open Vld) poursuit sa comparaison entre le système en vigueur aux Pays-Bas et celui qui est proposé par le projet de loi à l'examen, et se penche sur leur mise en œuvre respective.

Concrètement, la procédure aux Pays-Bas est la suivante:

1. l'inspecteur commence par formuler une enquête motivée;
2. l'instance concernée, par exemple une banque, juge si la demande est conforme au cadre légal;
3. en cas de doute, l'instance peut demander à l'inspecteur des précisions sur la portée de la demande;
4. les données sont transmises par des canaux numériques sécurisés.

Le membre précise qu'aux Pays-Bas, le fisc n'a pas le droit de mener des enquêtes à l'aveugle; chaque demande doit reposer sur un motif précis, tel qu'une irrégularité dans une déclaration ou une notification de l'unité de surveillance des opérations financières (Financial Intelligence Unit, ou FIU). Cette question relève des règles de proportionnalité et de subsidiarité.

En ce qui concerne le flux d'informations, les Pays-Bas jouent un rôle actif en matière d'échange automatique de données financières sur le plan international. Certaines conventions (CRS, FATC, etc.) amènent l'administration fiscale néerlandaise à recevoir chaque année une énorme quantité d'informations financières. Ces dernières doivent être traitées dans un environnement fermé et sécurisé, sous la supervision d'un fonctionnaire délégué à la protection des données – soit l'équivalent du DPO

DPO in België. De betreffende gegevens kunnen enkel worden gebruikt om aangiften en inningen te controleren; profilering of geautomatiseerde beoordeling zijn ten strengste verboden.

De Nederlandse FIU fungeert als tussenschakel tussen de financiële sector en de dienst voor het opsporen van verdachte transacties. Ze treedt op wanneer een bank ongebruikelijke transacties meldt op grond van de wet ter voorkoming van witwaspraktijken en het financieren van terrorisme. Als een transactie na een menselijke controle verdacht wordt geacht, wordt het dossier doorgestuurd naar het openbaar ministerie of het parket. De heer Van Quickenborne wijst er in dat verband op dat die gegevens niet automatisch worden meegedeeld aan de belasting- en douaneadministratie voor algemene risicoanalyse doeleinden. Een scheiding van de doeleinden werd juridisch vastgelegd.

De strijd tegen het witwassen van geld en belastingfraude valt onder twee afzonderlijke regimes. De Nationale Bank van Nederland (De Nederlandsche Bank – DNB) en de Nederlandse Autoriteit Financiële Markten (AFM), de twee toezichthoudende instellingen voor banken en verzekeringsmaatschappijen, oefenen ook een controle uit. De DNB en de AFM zien toe op de naleving van de financiële regels, maar houden geen toezicht op particulieren. Beide hebben toegang tot sectorgegevens, maar niet tot individuele klantgegevens. Alleen de FIU is gemachtigd de identiteit van rekeninghouders te koppelen aan transacties, en enkel in specifieke bestanden.

Daarnaast voert de Nederlandse belasting- en douaneadministratie een risicoselectie uit, wat een essentieel onderdeel vormt van de controle in Nederland. Sinds het begin van de jaren 2000 hanteert de Nederlandse belasting- en douaneadministratie de risicoselectie om te bepalen welke belastingaangiften nader moeten worden onderzocht. Het lid wijst erop dat België daartoe ook een beroep doet op datamining.

Datamining bestaat al een tijdje maar werd pas met de wet van 2012 echt in de Belgische wetgeving opgenomen. Volgens het lid zijn de door de minister beantwoorde parlementaire vragen de enige sporen die we daarvan hebben.

In Nederland gebeurt risicoselectie sinds het begin van de jaren 2000 op basis van algoritmen en statistische modellen. Het gaat hier niet om bankgegevens maar om verdachte situaties, zoals een plotselinge stijging van het inkomen of een onlogische combinatie van inkomsten en beroepskosten. Die factoren genereren risicoscores.

en Belgique. Les données en question ne peuvent être utilisées que pour le contrôle des déclarations et des encaissements; le profilage ou la notation automatisée sont strictement interdits.

La FIU des Pays-Bas assure quant à elle la liaison entre le secteur financier et le service de repérage des transactions suspectes. Elle intervient lorsqu'une banque signale des transactions inhabituelles en vertu de la loi relative à la prévention du blanchiment d'argent et du financement du terrorisme. Si, après vérification humaine, une transaction est jugée suspecte, le dossier est transmis au ministère public ou au parquet. M. Van Quickenborne souligne à ce sujet que ces données ne sont pas automatiquement communiquées à l'administration fiscale et douanière à des fins d'analyse générale des risques. Une séparation des finalités a été établie juridiquement.

La lutte contre le blanchiment et la fiscalité relèvent de deux régimes distincts. La Banque nationale néerlandaise (DNB) et l'Autorité néerlandaise des marchés financiers (AFM), les deux organismes de surveillance des banques et des compagnies d'assurance, exercent également un contrôle. La DNB et l'AFM veillent au respect de la réglementation financière, mais ne contrôlent pas les particuliers. L'une et l'autre ont accès aux données sectorielles, mais pas aux données individuelles des clients. Seule l'unité de surveillance (FIU) est autorisée à associer l'identité des titulaires de compte à des transactions, et uniquement dans des fichiers spécifiques.

Par ailleurs, l'administration fiscale et douanière néerlandaise procède à une sélection des risques, qui constitue un élément essentiel du contrôle aux Pays-Bas. Depuis le début des années 2000, l'administration fiscale et douanière néerlandaise utilise la sélection des risques pour déterminer quelles déclarations fiscales nécessitent un examen plus approfondi. Le membre signale que la Belgique a également recours à l'exploration de données à cette fin.

L'exploration de données, ou *data mining*, existe depuis un certain temps mais ce n'est qu'avec la loi de 2012 que cette pratique a été véritablement inscrite dans la législation belge. Selon le membre, les seules traces que nous en avons sont des questions parlementaires posées, auxquelles le ministre a répondu.

La sélection des risques au Pays-Bas se base, depuis le début des années 2000, sur des algorithmes et des modèles statistiques. Il n'est pas question de données bancaires, mais de situations suspectes, telles qu'une augmentation soudaine des revenus, ou une combinaison illogique de revenus et de dépenses professionnelles.

De uiteindelijke beslissing om een controle uit te voeren wordt echter altijd door mensen genomen.

In België daarentegen is er na de datamining bij de belastingdienst vrijwel geen menselijke tussenkomst meer. Auditoren die bestanden uit datamining ontvangen, zijn verplicht een audit uit te voeren en hebben geen enkele autonomie of discretionaire bevoegdheid meer om zich daartegen te verzetten.

De algoritmen zijn in feite gebaseerd op DAM-fiches (*Digital Access Management*). Als gevolg van de toeslagenaire in Nederland moeten beslissingen daar altijd door een mens worden genomen. Sinds 2021 geldt er een binnenlands beleid om de risico's op bias bij het gebruik van artificiële intelligentie te beperken. Daarom moet elke risicoselectie:

- gebaseerd zijn op een nauwkeurig omschreven wettelijke grondslag;
- worden onderworpen aan een ethische en evenredigheidstoetsing;
- worden gedocumenteerd om een latere audit mogelijk te maken.

Die controle wordt op haar beurt geverifieerd door de IBTD, de Nederlandse tegenhanger van de BBI.

Bovendien moet het gebruik van gegevens altijd worden onderworpen aan een gegevensbeschermingseffectbeoordeling (*Data Protection Impact Assessment*, DPIA), wat overeenkomt met de regelgevingsimpactanalyse (RIA) die in België wordt toegepast. Die beoordeling is wettelijk verplicht en bij elk wetsontwerp moet daarmee rekening worden gehouden.

Samengevat is de risicoselectie in Nederland op drie principes gebaseerd. Ten eerste moet controle gepaard gaan met risicobeheer. Ten tweede zijn menselijke controle en transparantie essentieel. Ten derde mag er geen datamining worden uitgevoerd bij bankgegevens. Dat betekent dat de Nederlandse belastingdienst geen toegang heeft tot banktransactiegegevens, behalve bij bepaalde specifieke individuele dossiers. Hij mag ook geen algoritmen toepassen op bankgegevens of er gebruiken voor het opstellen van profielen van particulieren.

Het lid buigt zich vervolgens over de juridische bescherming van de Nederlandse burgers met betrekking tot hun bankgegevens.

Ces éléments génèrent des scores de risque, mais la décision finale de procéder à une vérification revient toujours à des personnes.

En Belgique, par contre, il n'y a pratiquement plus d'intervention humaine suite à l'exploration de données au sein des autorités fiscales. Les auditeurs qui reçoivent des fichiers issus de l'exploration de données sont tenus de procéder à un audit et n'ont plus aucune autonomie, ni aucun pouvoir discrétionnaire pour s'y opposer.

Les algorithmes se basent en réalité sur des fiches DAM (*Digital Access Management*). Aux Pays-Bas, en raison du scandale des allocations familiales, il est impératif qu'une personne prenne toujours la décision. Depuis 2021, une politique interne est imposée pour limiter les risques de biais liés à l'utilisation de l'intelligence artificielle. Dès lors, toute sélection de risques doit:

- reposer sur une base légale décrite avec précision;
- faire l'objet d'un examen d'éthique et de proportionnalité;
- être documentée afin de permettre un audit ultérieur.

Ce contrôle est lui-même vérifié par l'équivalent de l'ISI aux Pays-Bas, l'IBTD.

En outre, l'utilisation de données doit toujours faire l'objet d'une analyse d'impact relative à la protection des données (*Data Protection Impact Assessment* – DPIA), qui correspond à l'analyse d'impact de la réglementation (AIR) pratiquée en Belgique. Cette analyse est prévue dans la législation et chaque projet de loi est censé en tenir compte.

En résumé, la sélection des risques, aux Pays-Bas, doit se fonder sur trois principes. Tout d'abord, le contrôle passe par la gestion des risques. Ensuite, le contrôle humain et la transparence sont essentiels. Et troisièmement, l'exploration de données bancaires est interdite. Cela signifie que l'administration fiscale néerlandaise n'a pas accès aux données de transactions bancaires, à l'exception de certains dossiers individuels spécifiques, et qu'il lui est interdit d'utiliser des algorithmes sur des données bancaires ou pour dresser des profils de particuliers.

Le membre se penche ensuite sur la protection juridique des citoyens néerlandais vis-à-vis de leurs données bancaires.

Ten eerste wordt in de Nederlandse wetgeving het recht van particulieren op informatie en toegang beschermd. Krachtens artikel 15 van de AVG hebben de burgers recht op toegang tot alle hen betreffende persoonsgegevens die de belasting- en douanediens of de financiële inlichtingendienst verwerkt. De regering moet binnen een termijn van vier weken op elk toegangsverzoek reageren. Bij weigering is er een beroepsmogelijkheid. De belasting- en douanediens kan tijdelijk informatie achterhouden als de openbaarmaking ervan een lopend onderzoek zou kunnen belemmeren, maar is verplicht de informatie later aan de burger door te geven zodra het onderzoek is afgerond.

Ten tweede heeft de Nederlandse burger recht op bezwaar, beroep of schadevergoeding. De heer Van Quickenborne vraagt zich af of een dergelijk recht ook in België bestaat. Kan men een klacht indienen bij de Gegevensbeschermingsautoriteit (GBA) en een schadevergoeding eisen op grond van artikel 82 van de AVG? En kunnen de betrokken ambtenaren in een dergelijk geval worden gestraft? Het lid benadrukt in dat verband dat in Nederland verschillende burgers een schadevergoeding hebben gekregen voor illegale profilering, met name in het kader van de voornoemde toeslagenaffaire, en dat dit heeft geleid tot structurele hervormingen van de toezichtprocedure.

Ten derde is de Nederlandse tegenhanger van de functionaris voor gegevensbescherming (DPO) belast met het interne toezicht op de naleving van de AVG. Hij rapporteert rechtstreeks aan de algemeen directeur en is onafhankelijk bij de uitoefening van zijn functies. Hij kan onderzoeken starten, waarschuwingen geven en processen opschorten als het risico bestaat dat de rechten op de bescherming van de persoonsgegevens worden geschonden.

Het lid beschrijft vervolgens de toeslagenaffaire, die in 2021 heeft geleid tot de val van de Nederlandse regering en aanleiding heeft gegeven tot een reeks controlemaatregelen. De heer Van Quickenborne wijst er ook op dat de Nederlandse GBA een boete van 3,7 miljoen euro heeft opgelegd aan het agentschap dat verantwoordelijk was voor dat schandaal. Sindsdien houdt datzelfde agentschap permanent toezicht op de gegevensverwerking binnen de belasting- en douanediens en moet elk project, algoritme of systeem vooraf worden gemeld.

Het lid is van oordeel dat de Belgische GBA ook klaarheid zou moeten scheppen over datamining door de federale overheid. Hij verwijst naar een schriftelijke vraag die hij op 24 maart 2025 over dit onderwerp aan de minister heeft gesteld om inzicht te krijgen in de werkwijze. Hij geeft toe dat de GBA niet het onderwerp van discussie

Premièrem, la législation néerlandaise protège le droit à l'information et d'accès des particuliers. En vertu de l'article 15 du RGPD, les citoyens ont le droit d'accéder à toutes les données personnelles traitées à leur sujet par l'administration fiscale et douanière ou par la cellule de renseignement financier (CRF). Le gouvernement doit répondre à toute demande en ce sens dans un délai de quatre semaines. Un droit de recours existe en cas de refus. L'administration fiscale et douanière peut temporairement retenir des informations si leur divulgation est susceptible d'entraver une enquête en cours, mais elle est tenue d'en informer le citoyen ultérieurement, une fois l'enquête terminée.

Deuxièmement, le citoyen néerlandais dispose d'un droit d'objection, de recours et d'indemnisation. M. Van Quickenborne se demande si un tel droit existe en Belgique. Peut-on porter plainte auprès de l'Autorité de protection des données (APD), et réclamer une indemnisation en vertu de l'article 82 du RGPD? Et les fonctionnaires concernés peuvent-ils être sanctionnés dans un tel cas? Le membre souligne à ce sujet qu'au Pays-Bas, plusieurs citoyens ont été indemnisés pour profilage illicite, notamment lors du scandale des allocations familiales évoqué plus haut, et que cela a conduit à des réformes structurelles de la procédure de contrôle.

Troisièmement, l'équivalent du délégué à la protection des données (DPO) aux Pays-Bas assure le suivi interne du respect du RGPD. Il relève directement du directeur général et est indépendant dans l'exercice de ses fonctions. Il peut lancer des enquêtes, émettre des avertissements et suspendre des processus en cas de risque de violation des droits à la protection des données personnelles.

Le membre décrit ensuite l'affaire des allocations familiales, qui a notamment donné lieu à la chute du gouvernement néerlandais en 2021 et à la prise d'une série de mesures de contrôle. M. Van Quickenborne indique également qu'une amende de 3,7 millions d'euros a été infligée par l'APD néerlandaise à l'agence responsable du scandale des allocations familiales. Et depuis lors, cette même agence surveille en permanence le traitement des données au sein de l'administration fiscale et douanière et tout nouveau projet, algorithme ou système doit être notifié au préalable.

Pour le membre, l'APD en Belgique devrait elle aussi faire la lumière sur l'exploration de données effectuée par le gouvernement fédéral. Il se réfère à une question écrite qu'il a posée au ministre à ce sujet le 24 mars 2025, afin de comprendre comment cela fonctionne. Il admet que l'APD n'est pas le sujet de discussion mais

is, maar wijst erop dat die instantie werd verzocht om een advies uit te brengen over het wetsontwerp en de amendementen die hier worden besproken. Het advies in kwestie was heel negatief. Het lid leidt daaruit af dat de GBA geen voorstander is van het gebruik van data-mining. In tegenstelling tot wat in Nederland het geval is, heeft de GBA echter slechts beperkte zeggenschap in die aangelegenheid.

De heer Van Quickenborne verwijst vervolgens naar het debat dat in 2018 werd gevoerd over de wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van rekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest. Hij herinnert eraan dat de GBA toen een advies¹ heeft uitgebracht met een reeks bezwaren waaraan telkens gevolg werd gegeven in de amendementen op het wetsontwerp in kwestie. Hij betreurt daarom dat ditmaal geen rekening wordt gehouden met de bezwaren van de GBA over dit wetsontwerp.

Sinds de “toeslagenaffaire” voorziet het Nederlandse recht in een verplichting dat een persoon steeds de beslissing moet nemen. Elke risicoselectie dient op een juridische grondslag te berusten. Voorts wordt de proportionaliteit getoetst. Tot slot wordt er gedocumenteerd om controle achteraf mogelijk te maken en wel door de Inspectie Belastingen, Toeslagen en Douane. Voor de datatoepassing geldt dan een “data protection impact assessment”. Datamining van bankgegevens is vooralsnog niet geoorloofd en men lijkt ook niet van plan om de wet in die zin aan te passen.

De spreker verwijst naar zijn voormalige functie als staatssecretaris en beschrijft de Kafkatoets die hij destijds had ingevoerd. Probleem bij de Reguleringssimpactanalyse (RIA) die de eerdere – veeleer beknopte – toets zou vervangen, is dat die vaak onverteerbaar is, mede door de omvang. De werkwijze kan men doorgaans ook niet ernstig noemen.

Het lid bespreekt vervolgens de rechtspositie van de burger in Nederland ten aanzien van de behandelde problematiek en citeert om te beginnen artikel 15 van de Algemene Verordening Gegevensbescherming (AVG), dat het recht van inzage verleent in het kader van de behandeling van persoonsgegevens door de belastingdienst die de betrokkene betreffen. Daarbij dient de overheid een bepaalde termijn in acht te nemen om te antwoorden op een verzoek (vier weken). Bij weigering biedt de wet de mogelijkheid om in beroep te gaan.

¹ <https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-15-2018.pdf>

rappelle que cette instance a été sollicitée pour fournir un avis au sujet du projet de loi et des amendements à l'examen. L'avis en question s'est révélé très négatif. Le membre en déduit que l'APD n'est pas favorable à l'utilisation du *data mining*. Cependant, contrairement à la situation aux Pays-Bas, l'APD n'a qu'un droit de regard limité sur cette question.

M. Van Quickenborne se réfère ensuite au débat mené en 2018 concernant la loi du 8 juillet 2018 relative à l'organisation d'un point de contact central pour les comptes et les contrats financiers et à l'extension de l'accès au fichier central des avis de saisie, de délégation, de transfert, de règlement collectif de dettes et de protêt. Il rappelle que l'APD avait alors émis un avis¹ rassemblant une série d'objections, qui ont toutes été prises en compte dans les amendements au projet de loi en question. Il regrette dès lors que les objections de l'APD sur le projet de loi à l'examen ne soient pas prises en considération cette fois-ci.

Depuis “l'affaire des allocations familiales”, le droit néerlandais impose que la décision soit toujours prise par une personne. Toute sélection des risques doit reposer sur une base juridique. En outre, il faut prévoir un contrôle de proportionnalité. Enfin, la décision doit être documentée pour permettre un contrôle *a posteriori* par l'Inspectie Belastingen, Toeslagen en Douane). L'application des données doit être soumise, quant à elle, à une “analyse d'impact relative à la protection des données”. Le *data mining* des données bancaires n'est pas autorisé pour l'instant et tout semble indiquer que l'intention n'est pas de modifier la loi en ce sens.

L'intervenant évoque la fonction qu'il a exercée auparavant en tant que secrétaire d'État et décrit le Test Kafka qu'il avait instauré à l'époque. Le problème de l'analyse d'impact de la réglementation (AIR) qui devait remplacer le contrôle précédent – plutôt concis –, est que celle-ci est souvent indigeste, en partie à cause de son ampleur. Quant à la méthode, elle ne peut généralement pas être qualifiée de sérieuse.

L'intervenant commente ensuite la position juridique du citoyen néerlandais en ce qui concerne la problématique traitée et rappelle d'abord l'article 15 du Règlement général sur la protection des données (RGPD) qui accorde à la personne concernée le droit d'accès lorsque des données à caractère personnel la concernant sont traitées par l'administration fiscale. À cet égard, l'administration est tenue de respecter un délai précis pour répondre à une demande (quatre semaines). En cas de refus, la loi prévoit la possibilité d'introduire un recours. Ces

¹ <https://www.autoriteprotectiondonnees.be/publications/avis-n-15-2018.pdf>

Het tijdelijk achterwege laten van informatie wordt op basis van een aantal criteria toegestaan, zoals het feit dat openbaarmaking het onderzoek zou belemmeren, maar na afronding van een onderzoek heeft de burger evenwel recht op informatie.

Waar bezwaar, beroep en schadevergoeding in het Nederlandse recht zijn verankerd, is het de vraag of dezelfde rechten in België bestaan. In Nederland werd burgers immers schadevergoeding toegekend wegens onrechtmatige profilering in de “toeslagenaffaire”, wat tot structurele hervormingen heeft geleid in het toezicht.

De Functionaris Gegevensbescherming (FG) vervult een essentiële rol in de waarborging van de rechtsbescherming van burgers in Nederland. Elke overheid beschikt er over een FG, wat allicht overeenkomt met de *data protection officer* (DPO) in België. Hij houdt toezicht op de naleving van de AVG. De spreker licht zijn rol en bevoegdheden nader toe.

In Nederland wordt bovendien nog een controle uitgevoerd. Het lid verwijst naar de Autoriteit Persoonsgegevens (AP) die in een rapport van 2021 onrechtmatigheden aan de kaak stelt. Zo werden jarenlang persoonsgegevens verwerkt, waaronder de nationaliteit, zonder wettelijke basis. Dat heeft een schok veroorzaakt die tot de val van de regering heeft geleid (*infra*).

De AP (te vergelijken met de Gegevensbeschermingsautoriteit GBA) heeft zelfs een boete opgelegd aan de Nederlandse Belastingdienst van 3,7 miljoen euro, de dienst verantwoordelijk voor de “toeslagenaffaire”. Hoe moet men zich die boete eigenlijk concreet voorstellen?

Maar het feit heeft weerklank gevonden, tot voorbij de Nederlandse grenzen. Dat is zonder twijfel een positieve ontwikkeling. Sindsdien voert de AP in Nederland permanent toezicht uit op de verwerking van persoonsgegevens binnen de Belastingdienst. Elk nieuw project, algoritme of systeem moet vooraf worden gemeld.

Het zou dan ook wenselijk zijn dat de Belgische Gegevensbeschermingsautoriteit (GBA) haar aandacht zou kunnen richten op de datamining die door de Belgische overheid wordt bedreven. Want dat blijft een van de grootste mysteries. Op 24 maart 2025 heeft

informations peuvent être omises provisoirement moyennant le respect de certains critères, comme le fait que leur divulgation entraverait l'enquête. Une fois l'enquête clôturée, le citoyen a toutefois le droit d'être informé.

Alors que le droit de faire opposition, d'introduire un recours et de réclamer des dommages et intérêts sont ancrés dans le droit néerlandais, on peut se demander si les mêmes droits existent en Belgique. Dans “l'affaire des allocations”, des citoyens ont en effet été indemnisés par les autorités néerlandaises pour profilage illicite, ce qui a entraîné des réformes structurelles en matière de surveillance.

Le *Functionaris Gegevensbescherming* (FG) (délégué à la protection des données) remplit un rôle essentiel en ce qui concerne la protection juridique des citoyens aux Pays-Bas. Chaque autorité publique y possède son FG, lequel est, en Belgique, dénommé Délégué à la protection des données (DPD). Sa mission consiste à contrôler le respect du RGPD. L'intervenant commente son rôle et ses compétences plus en détail.

En outre, les Pays-Bas ont instauré un contrôle supplémentaire. Le membre évoque l'Autoriteit Persoonsgegevens (l'Autorité de protection des données néerlandaise, AP) qui, dans un rapport publié en 2021, a dénoncé des irrégularités. Ainsi, des années durant, des données à caractère personnel, telles que la nationalité, ont été traitées sans base légale. Ce constat a provoqué un choc qui a conduit à la chute du gouvernement (*cf. infra*).

L'AP (comparable à notre Autorité de protection des données – APD) a même infligé une amende de 3,7 millions d'euros à l'administration fiscale néerlandaise, responsable du scandale des allocations familiales. Comment se représenter la mise en œuvre concrète de ce mécanisme d'amende?

Cet événement a toutefois fait écho au-delà des frontières néerlandaises, ce qui constitue sans aucun doute une évolution positive. Depuis lors, aux Pays-Bas, l'AP exerce un contrôle permanent sur le traitement des données à caractère personnel au sein de l'administration fiscale. Tout nouveau projet, algorithme ou système doit être signalé au préalable.

Il serait donc souhaitable que l'Autorité belge de protection des données (APD) puisse se pencher sur le *data mining* pratiqué par les autorités belges. Car nous sommes ici face à un très grand mystère. Le 24 mars 2025, le membre a adressé une question écrite à ce

het lid hierover een schriftelijke vraag gericht de bevoegde minister, met het verzoek om opheldering over de werking van deze praktijken.

Hoe dan ook, de GBA heeft een vernietigend advies gegeven met betrekking tot voorliggend wetsontwerp. Mocht de GBA zich ook eens kunnen uitspreken over datamining, dan zou dat heel verrijkend kunnen zijn.

In 2018 heeft de voormalige minister van Financiën advies verkregen van de toenmalige Privacycommissie. Die heeft elf adviezen verstrekt, waarmee rekening werd gehouden. Indien de huidige minister van Financiën dezelfde methode had willen volgen, zou de huidige bespreking sneller kunnen verlopen.

Het probleem is dat de regering zich nadrukkelijk blijft verzetten tegen het uiterst kritische advies, louter omdat één partij binnen de coalitie – de socialistische fractie Vooruit – erop aandringt dat het wetsontwerp wordt aangenomen. Dat verklaart overigens ook het manoeuvre met de amendementen: binnen één uur werden de amendementen ingediend, vervolgens weer ingetrokken na protest van de liberale fractie MR en anderen, en daarna opnieuw ingediend.

Hoe oefent Nederland controle uit? Veel proactiever dan België, in ieder geval. Het lid vergelijkt de werking van een uitgedunde Kamercommissie van Financiën met het gewicht van de Nederlandse commissies Financiën, Digitale Zaken en Justitie en Veiligheid. De Nederlandse Tweede Kamer ontvangt jaarlijks een privacyverslag van de Belastingdienst en bespreekt dat in openbare hoorzittingen. En de Nationale Ombudsman speelt een belangrijke rol bij klachten over de fiscale aangelegenheden. Het Nederlandse voorbeeld is beslist indrukwekkend.

De spreker weigert zich bij de gang van zaken in België neer te leggen.

In Nederland beschikt de Algemene Rekenkamer over de bevoegdheid om toezicht uit te oefenen op de naleving van het beginsel van behoorlijk bestuur bij de verwerking van persoonsgegevens door de Belastingdienst. Dat model verdient aandacht.

Een vergelijkbare aanpak zou ook in België kunnen worden overwogen, waarbij het Rekenhof een toezichthoudende rol krijgt inzake dataverwerking binnen de federale administratie.

Het toekennen van deze bevoegdheid zou een belangrijke stap zijn richting versterkte rechtsbescherming en

sujet au ministre compétent, lui demandant des éclaircissements sur le fonctionnement de ces pratiques.

Quoi qu'il en soit, l'APD a rendu un avis accablant sur le projet de loi à l'examen. Il serait très utile que l'Autorité puisse également se prononcer sur le *data mining*.

En 2018, le ministre des Finances de l'époque avait consulté l'ex-Commission de la protection de la vie privée, qui avait formulé 11 avis au total. Ces avis avaient été pris en considération. Si l'actuel ministre des Finances avait voulu suivre la même méthode, les discussions actuelles auraient pu avancer plus rapidement.

Le gouvernement actuel continue toutefois de s'opposer fermement à cet avis extrêmement critique, au seul motif qu'un parti de la coalition – le groupe socialiste Vooruit – insiste pour que le projet de loi soit adopté. Le stratagème mis en place avec les amendements en est aussi la parfaite illustration: ces amendements ont été présentés en l'espace d'une heure, puis retirés après les protestations du groupe libéral MR et d'autres, avant d'être à nouveau présentés.

Comment les Pays-Bas exercent-ils leur contrôle? De manière bien plus proactive que la Belgique, en tout cas. Le membre compare le fonctionnement d'une commission des Finances diluée de la Chambre au poids des commissions néerlandaises des Finances, des Affaires numériques ainsi que de la Justice et de la Sécurité. La Tweede Kamer des Pays-Bas reçoit chaque année un rapport de l'administration fiscale sur la protection de la vie privée et en discute lors d'auditions publiques. Par ailleurs, le Médiateur national joue un rôle important dans le traitement des plaintes relatives aux questions fiscales. L'exemple néerlandais fait assurément forte impression.

L'intervenant refuse de cautionner la tournure que prend actuellement la politique belge.

Aux Pays-Bas, la Cour des comptes (Algemene Rekenkamer) est habilitée à contrôler le respect du principe de bonne gouvernance dans le traitement des données à caractère personnel par l'administration fiscale. Ce modèle mérite d'être examiné plus avant.

Une approche similaire pourrait également être envisagée en Belgique. La Cour des comptes serait ainsi amenée à surveiller le traitement des données au sein de l'administration fédérale.

L'octroi de cette compétence constituerait une avancée importante vers un renforcement de la protection juridique

verantwoord datagebruik binnen de overheid. Dergelijke modaliteiten kunnen het debat over digitale transparantie en bestuurlijke verantwoordelijkheid een duidelijke richting geven.

Vooralsnog blijft het echter stil. Er is geen vooruitgang, enkel afwachten in de hoop dat de discussie vanzelf verdwijnt. Maar dat zal niet gebeuren.

In Nederland is de Inspectie Belastingen, Toeslagen en Douane (IBTD) actief. Deze instantie houdt toezicht op de naleving van regelgeving binnen de fiscale en douane-administratie. Daarnaast publiceert de inspectie thematische rapporten over risico's in data-analyse en privacy, waarmee ze bijdraagt aan transparantie en verantwoord datagebruik.

Zowel de IBTD als de Algemene Rekenkamer hebben herhaaldelijk benadrukt dat de Nederlandse Belastingdienst sinds de invoering van dit toezicht aanzienlijke vooruitgang heeft geboekt op het vlak van *governance* en transparantie.

Het roept de vraag op waarom een soortgelijk model niet kan worden toegepast in België.

Het lid analyseert de SyRI-uitspraak betreffende het systeem risico-indicatie. De rechtbank van Den Haag verklaarde in februari 2020 dat het systeem risico-indicatie – een algoritmisch model dat in Nederland werd toegepast – onrechtmatig was wegens schending van artikel 8 van het EVRM. SyRI koppelde gegevens uit verschillende overheidsdatabanken met het oog op fraudebestrijding.

De rechtbank stelde vast dat de gebruikte algoritmen onvoldoende transparant, onvoldoende controleerbaar en onvoldoende voorzien waren van waarborgen tegen willekeur.

Er rijst dan ook de vraag of de algoritmen die hier worden toegepast voldoende transparant zijn, voldoende controleerbaar en voldoende waarborgen bieden tegen willekeur.

Het arrest heeft een grote precedentswaarde in Nederland. Men is er sindsdien immers van overtuigd dat datamining door de overheid in strijd is met de grondrechten.

De kinderopvangtoeslagenaffaire in Nederland leidde tot een parlementair onderzoek. De parlementaire onderzoekscommissie bracht aan het licht dat de

et vers une utilisation responsable des données au sein de l'administration. Les modalités de cette compétence pourraient clairement orienter le débat sur la transparence numérique et la responsabilité administrative.

L'immobilisme demeure toutefois pour l'instant. Plutôt que d'avancer, on se contente d'attendre dans l'espoir que la discussion s'éteigne d'elle-même. Or, cela n'arrivera pas.

Aux Pays-Bas, l'Inspection des impôts, des surtaxes et des douanes (Inspectie Belastingen, Toeslagen en Douane (IBTD)) contrôle le respect de la réglementation au sein de l'administration fiscale et douanière. Elle publie en outre des rapports thématiques sur les risques liés à l'analyse des données et au respect de la vie privée, contribuant ainsi à la transparence et à une utilisation responsable des données.

Tant l'IBTD que l'Algemene Rekenkamer ont souligné à plusieurs reprises que, depuis l'instauration de ces contrôles, l'administration fiscale néerlandaise avait considérablement progressé en matière de gouvernance et de transparence.

Il convient de se demander pourquoi un modèle similaire ne pourrait pas être appliqué en Belgique.

Le membre analyse ensuite la décision judiciaire rendue concernant le *systeem risico-indicatie* ou SyRI (système de traitement automatique des données pour détecter la fraude). En février 2020, le tribunal de La Haye a déclaré que le modèle algorithmique appliqué aux Pays-Bas était illégal dès lors qu'il violait l'article 8 de la CEDH. Ce système reliait les données provenant de différentes banques de données publiques dans le but de détecter la fraude.

Le tribunal a estimé que les algorithmes utilisés n'étaient pas suffisamment transparents ni contrôlables et qu'ils n'offraient pas de garanties suffisantes pour éviter l'arbitraire.

Il convient dès lors de se demander si les algorithmes appliqués en Belgique seront suffisamment transparents et contrôlables et s'ils offriront suffisamment de garanties pour éviter l'arbitraire.

Cet arrêt représente un précédent de taille aux Pays-Bas, où l'on est désormais convaincu que le *data mining* pratiqué par les autorités publiques contrevient aux droits fondamentaux.

Dans ce pays, le scandale des allocations de garde d'enfants a fait l'objet d'une enquête parlementaire. La commission d'enquête parlementaire a mis en lumière

Belastingdienst gedurende meerdere jaren risicoselecties uitvoerde op basis van nationaliteit en onduidelijke criteria. De Nederlandse overheid heeft deze praktijk uiteindelijk erkend.

De affaire werd door de overheid aangemerkt als een ernstige schending van het gelijkheidsbeginsel (artikel 1 van de Grondwet), het recht op eerbiediging van de persoonlijke levenssfeer (artikel 10 van de Grondwet), en het verbod op automatische besluitvorming zoals vastgelegd in artikel 22 van de Algemene Verordening Gegevensbescherming (AVG).

De gevolgen waren ingrijpend: de val van het kabinet Rutte III, een volledige herstructurering van de Belastingdienst, en de invoering van strikte regels voor data-analyse en risicoselectie.

Waarom wacht men in België – een privacymonster – toch steeds af tot de zaken verkeerd lopen om in te grijpen? Het land moet leren uit de toeslagenaffaire. Het lid vraagt op welke wijze de minister daarmee rekening zal houden. Men moet zich hoeden voor de beknotting van de vrijheid door de wet.

Algemene gegevensbewaring, profilering en risicomechanismen die gelden voor alle burgers worden beschouwd als onverenigbaar met de artikelen 7 en 8 van het Handvest van de Grondrechten van de Europese Unie.

Deze principes worden bevestigd in parlementaire debatten en beleidsdocumenten van het ministerie van Justitie en Veiligheid. Er zijn diverse documenten die dit onderbouwen, maar die worden op dit moment niet geciteerd, aangezien het dossier nog in behandeling is.

In Nederland wordt met deze kwesties aanzienlijk zorgvuldiger omgegaan. Dat land heeft eerst een affaire beleefd en daaruit lessen getrokken.

Bij een vergelijking tussen België en Nederland valt op dat het Nederlandse systeem gedecentraliseerd is, terwijl het Belgische systeem gecentraliseerd functioneert. In België berust het beheer bij de Nationale Bank van België. In Nederland zijn meerdere instanties betrokken, waaronder de Belastingdienst, De Nederlandsche Bank en de Financial Intelligence Unit (FIU).

In Nederland worden enkel relevante gegevens per dossier verwerkt; in België worden systematisch alle rekeningen en contracten geraadpleegd. Toegang tot gegevens is in Nederland gericht en gemotiveerd, terwijl in België brede toegang wordt gehanteerd. Profilering is

que l'administration fiscale avait, des années durant, procédé à une sélection des risques sur la base de la nationalité et de critères flous. Les autorités publiques néerlandaises ont fini par reconnaître cette pratique.

Elles ont considéré que cette affaire représentait une grave violation du principe d'égalité (article 1^{er} de la Constitution), du droit au respect de la vie privée (article 10 de la Constitution) et de l'interdiction des décisions fondées exclusivement sur un traitement automatisé prévue à l'article 22 du Règlement général sur la protection des données (RGPD).

Les conséquences ont été dramatiques: chute du gouvernement Rutte III, restructuration complète de l'administration fiscale et introduction de règles strictes en termes d'analyse des données et de sélection des risques.

Pourquoi la Belgique – un pays obsédé par le respect de la vie privée – continue-t-elle à attendre une catastrophe pour intervenir? Notre pays doit tirer les leçons de l'affaire des allocations de garde d'enfants. Le membre demande comment le ministre en tiendra compte. Il faut éviter que la loi ne vienne restreindre les libertés.

La conservation générale des données, le profilage et les mécanismes de sélection des risques sont considérés comme incompatibles avec les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

Ces principes sont confirmés par des débats parlementaires et par des documents politiques du ministère de la Justice et de la Sécurité. Plusieurs textes étayaient cette analyse, mais ils ne sont pas cités pour l'instant puisque le dossier est encore à l'examen.

Les Pays-Bas se montrent beaucoup plus prudents à l'égard de ces problématiques. Ce pays a vécu un premier scandale et en a retiré les enseignements qui s'imposaient.

Si l'on compare les deux pays, on constate que le système néerlandais fonctionne de manière décentralisée tandis que le système belge est, au contraire, centralisé. Chez nous, la gestion est confiée à la Banque nationale de Belgique. Aux Pays-Bas, plusieurs instances, comme l'administration fiscale, la Nederlandsche Bank et la Financial Intelligence Unit (FIU) sont impliquées.

Aux Pays-Bas, seules les données pertinentes sont traitées dans un dossier particulier; en Belgique, tous les comptes et tous les contrats sont systématiquement scrutés. Aux Pays-Bas, l'accès aux données est ciblé et motivé tandis qu'en Belgique, l'administration

in Nederland wettelijk verboden, in België toegestaan in het kader van *money control*.

De menselijke toets is in Nederland verplicht en bestaat uit meerdere stappen. In België is deze toetsing beperkt.

Toezicht in Nederland wordt uitgeoefend door een sterke Autoriteit Persoonsgegevens, met parlementaire en gerechtelijke verankering. In België ontbreekt een vergelijkbare structuur.

Sinds 2012 is de minister van Financiën wettelijk verplicht jaarlijks verslag uit te brengen over de werking van het KAP, zowel juridisch als technisch. Tot op heden is geen verslag ontvangen, ondanks herhaalde verzoeken vanuit de commissie. De wettelijke bepaling wordt structureel niet nageleefd.

In Nederland wordt wetgeving vergezeld van evaluatiemomenten en soms voorzien van een *sunset clause*, waarbij regelgeving automatisch vervalt tenzij hernieuwd. Dit draagt bij aan vereenvoudiging en rechtszekerheid.

In Nederland vertrekt controle vanuit vertrouwen in de burger en wordt enkel toegepast bij concrete aanwijzingen. In België vertrekt controle vanuit wantrouwen, waarbij preventieve algoritmische screening als efficiëntiemodel wordt gepresenteerd.

Het Belgische model is structureel gevoelig voor misbruik. In Nederland is het juridisch ontworpen om misbruik te voorkomen.

Ondanks beperkte bevoegdheden ligt de compliancegraad in Nederland op 95 %, tegenover 88 % in België. Ervaringen tonen aan dat rechtszekerheid, vertrouwen en transparantie de naleving van fiscale regels bevorderen. Een gebrek aan transparantie ondermijnt het vertrouwen in de overheid.

Nederland voldoet aan de drie proportionaliteitscriteria: geschiktheid (enkel effectief toezicht), noodzakelijkheid (toepassing in concrete gevallen), en evenredigheid (beperkte inbreuk). Het Nederlandse model garandeert dat de Staat niet meer weet dan noodzakelijk. België evolueert naar een systeem waarin de staat meer weet dan nodig is, wat een risico vormt op een overmatige, centraliserende controle.

Het Nederlandse model toont aan dat transparantie niet gelijk hoeft te staan aan surveillance, mits bevoegdheden strikt worden verankerd en gegevensuitwisseling

dispose d'un accès étendu. La loi néerlandaise interdit le profilage; la loi belge l'autorise dans le cadre de sa législation *money control*.

Le mécanisme néerlandais impose une intervention humaine à plusieurs étapes du processus. En Belgique, ce contrôle humain reste limité.

Aux Pays-Bas, le contrôle est exercé par une autorité de protection des données à caractère personnel robuste, disposant d'un ancrage parlementaire et judiciaire. La Belgique ne possède pas de structure comparable.

Depuis 2012, la loi impose au ministre des Finances de faire rapport chaque année sur le fonctionnement du PCC, sur le plan juridique comme sur le plan technique. À ce jour, aucun rapport n'a été reçu, malgré les demandes répétées de la commission. Cette disposition légale est structurellement ignorée.

Aux Pays-Bas, la législation est assortie de moments d'évaluation et, parfois, d'une *sunset clause*, par laquelle une réglementation expire automatiquement à moins d'être renouvelée. Cela contribue à la simplification et à la sécurité juridique.

Aux Pays-Bas, les autorités adoptent un principe de confiance envers le citoyen et ne procèdent au contrôle qu'en présence de signaux concrets. En Belgique, en revanche, les autorités appliquent un principe de méfiance et présentent la sélection algorithmique préventive comme un modèle d'efficacité.

Le modèle belge est, par nature, sensible aux fraudes. Aux Pays-Bas, il a été conçu juridiquement pour prévenir les abus.

Malgré des pouvoirs limités, le système néerlandais affiche un taux de conformité de 95 %, contre 88 % en Belgique. L'expérience a démontré que la sécurité juridique, la confiance et la transparence favorisaient le respect des règles fiscales. Un manque de transparence fragilise la confiance envers les autorités publiques.

Les Pays-Bas répondent aux trois critères de proportionnalité: adéquation (contrôle effectif uniquement), nécessité (application dans des cas concrets) et proportionnalité (atteinte limitée à la vie privée). Le modèle néerlandais garantit que l'État n'en sait pas plus que nécessaire. La Belgique évolue vers un système où l'État aura accès à trop d'informations, ce qui risque de conduire à un contrôle excessif et centralisé.

Le modèle néerlandais démontre que transparence ne doit pas forcément aller de pair avec surveillance, pour autant que les compétences des autorités soient

beperkt blijft tot concrete gevallen. De essentie van het Nederlandse model is dat controle de uitzondering vormt, niet de regel. België dreigt van deze uitzondering een regel te maken, met alle risico's van dien.

De heer Lode Vereeck (VB) acht het nuttig om de toeslagenaffaire ter sprake te brengen in het debat. Men dient te beseffen dat de geautomatiseerde gegevensverwerking in Nederland heel wat gezinnen heeft gebroken, met bijzonder zware sociale en financiële gevolgen voor de betrokkenen. Het lid treedt de vorige spreker op dat punt bij: men mag die zaak niet zomaar negeren.

De heer Vincent Van Quickenborne (Open Vld) gaat vervolgens in op het vierde – Zweedse – model. Zweden neemt binnen Europa een unieke positie in op het vlak van transparantie, administratief vertrouwen en gegevensbeheer. Terwijl veel landen in de voorbije decennia kozen voor centralisatie en uitbreiding, koos Zweden voor een gecontroleerde openheid die diep verankerd is in de nationale rechtscultuur.

Het Zweedse model steunt op twee fundamentele principes: het *offentlighetsprincipen*, het grondwettelijke principe van openbaarheid van bestuur, en het *integritetsskydd*, het recht op persoonlijke levenssfeer. Deze twee waarden – openheid en bescherming – lijken op het eerste gezicht tegenstrijdig, maar worden in Zweden op een complementaire manier toegepast. Het resultaat is een stelsel waarin de overheid beschikt over efficiënte instrumenten voor fiscale controle en witwasbestrijding, zonder dat burgers worden onderworpen aan massale dataverzameling of geautomatiseerde profilering.

Historisch gezien is de Zweedse fiscaliteit gebaseerd op het idee dat belastingheffing een collectieve verantwoordelijkheid is. Al sinds de jaren zeventig zijn de inkomens en belastinggegevens van burgers in Zweden publiek toegankelijk. Iedere burger kan via de *Skatteverket*, de Zweedse belastingdienst, iemands inkomen en belastingbedrag opvragen. Deze praktijk is geworteld in het voormelde grondwettelijke principe van openbaarheid van bestuur, zoals vastgelegd in de *Tryckfrihetsförordningen*, de persvrijheidswet van 1949. De publieke toegankelijkheid van deze gegevens dient niet om burgers te controleren, maar om maatschappelijke transparantie en gelijke behandeling te waarborgen.

Ook in Nederland worden er stappen in die richting gezet: het kadastraal inkomen van woningen is er publiek raadpleegbaar. In België is dat gelukkig niet het geval. De spreker meent dat de bron van dergelijke beslissingen inzake openbaarheid in Zweden ligt. Tegelijkertijd

strictement definiëerd en dat de uitwisselingen van gegevens beperkt blijven tot concrete gevallen. De essentie van het Nederlandse model is dat controle de uitzondering vormt, niet de regel. En België, deze uitzondering zou kunnen worden de regel, met alle risico's die hieraan verbonden zijn.

M. Lode Vereeck (VB) juge utile d'intégrer la question du scandale des allocations de garde d'enfants au débat. Il est important de comprendre que le traitement automatisé des données a brisé de nombreuses familles néerlandaises, confrontées à de graves conséquences sociales et financières. Le membre rejoint l'intervenant précédent sur ce point: cette affaire ne peut pas être ignorée.

M. Vincent Van Quickenborne (Open Vld) aborde, en quatrième lieu, le modèle suédois. La Suède présente un profil unique en Europe en matière de transparence, de confiance administrative et de gestion des données. Alors que de nombreux pays ont opté pour la centralisation et l'extension au cours des dernières décennies, la Suède a fait le choix d'une publicité contrôlée, profondément ancrée dans la culture juridique nationale.

Le modèle suédois repose sur deux principes fondamentaux: le principe constitutionnel de la publicité de l'administration (*offentlighetsprincipen*) et le droit à la vie privée (*integritetsskydd*). La publicité et la protection sont deux valeurs qui semblent contradictoires à première vue, mais qui sont appliquées de manière complémentaire en Suède. Il en résulte un système dans lequel les pouvoirs publics disposent d'instruments efficaces pour le contrôle fiscal et la lutte contre le blanchiment, sans que les citoyens ne soient soumis à une collecte massive de données ni à un profilage automatisé.

D'un point de vue historique, la fiscalité suédoise se base sur l'idée que la taxation constitue une responsabilité collective. Les revenus et les données fiscales des citoyens ont été rendus publics en Suède dès les années septante. Par le biais de l'administration fiscale suédoise (*Skatteverket*), chaque citoyen peut consulter le revenu d'une personne et le montant des impôts qu'elle paie. Cette pratique est enracinée dans le principe constitutionnel précité de la publicité de l'administration, défini dans la loi sur la liberté de la presse de 1949 (*Tryckfrihetsförordningen*). La publicité de ces données ne sert pas à contrôler les citoyens, mais à garantir la transparence sociétale et l'égalité de traitement.

Des mesures similaires sont également prises aux Pays-Bas, où les données relatives au revenu cadastral des logements sont accessibles au public. Ce n'est heureusement pas le cas en Belgique. L'intervenant estime que les décisions de ce type en matière de

gelden in dat land strikte beperkingen op de verwerking van persoonsgegevens door de overheid zelf.

Na deze eerste fase van openbaarmaking van gegevens werd in een tweede fase de overheid gemoderniseerd. Zo werd de Zweedse fiscale administratie al in de jaren negentig grondig gedigitaliseerd, terwijl dat in België pas gebeurde onder het toenmalig ministerschap van de heer Didier Reynders. De Zweedse belastingdienst is aldus geëvolueerd tot een geïntegreerde digitale organisatie die alle aangiften elektronisch beheert. Banken werden verplicht om jaarlijks geaggregeerde gegevens over rente, dividenden en hypotheekschulden te rapporteren. Deze rapportering gebeurt niet realtime maar jaarlijks, met het oog op de belastingheffing en niet op een permanente monitoring.

In een derde fase werden hervormingen doorgevoerd in het kader van initiatieven van de Europese Unie en de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO). Zo werd in 1998 de *Personuppgiftslagen* ingevoerd, de eerste nationale wet die de verwerking van persoonsgegevens regelde, in overeenstemming met de toen geldende Europese Richtlijn 95/46/EG. Deze wet legde de basis voor de latere Zweedse uitvoeringswet bij de Algemene Verordening Gegevensbescherming (AVG). Sinds 2010 heeft Zweden daarnaast de *Common Reporting Standards* van de OESO en de Europese antiwitwasrichtlijnen (AMLD) ingevoerd. Het land voerde tevens een nationaal rekeningregister in. Met dat *Kontoregister*, dat uitsluitend door de banken zelf en niet door de overheid wordt beheerd, worden banken verplicht rekeningnummers te koppelen aan de overeenstemmende rekeninghouders.

De *Finansinspektionen* (FI), de Zweedse financiële toezichthouder, ziet toe op de naleving van de antiwitwasverplichtingen en rapporteert aan de *Finanspolisen*, de Zweedse financiële inlichtingeneenheid (FIU), die vergelijkbaar is met de Belgische Cel voor Financiële Informatieverwerking (CFI). De Zweedse belastingdienst ontvangt enkel de financiële gegevens die strikt noodzakelijk zijn voor de belastingheffing, en dit uitsluitend binnen het kader van de *Skatteförfarandelagen* (SFL), de wet op de fiscale procedures.

Sinds 2017 geldt in Zweden ook een nationale wet inzake maatregelen tegen het witwassen van geld en de financiering van terrorisme (*Lag om åtgärder mot penningtvätt och finansiering av terrorism*), waarmee de EU-Richtlijnen 2015/849 en 2018/843 werden omgezet. Ook die wet bevat geen bepalingen die datamining door de overheid toelaten.

publicité trouvent leur source en Suède. Dans ce pays, le traitement des données à caractère personnel par les autorités elles-mêmes est par ailleurs strictement balisé.

Cette première phase prévoyant la publication des données a été suivie par une deuxième, qui visait une modernisation des pouvoirs publics. L'administration fiscale suédoise a été profondément numérisée dès les années nonante, alors que ce processus n'a eu lieu en Belgique qu'à l'époque où M. Didier Reynders était ministre des Finances. L'administration fiscale suédoise est ainsi devenue une organisation numérique intégrée qui gère toutes les déclarations de manière électronique. Les banques ont été tenues de fournir chaque année des données agrégées sur les intérêts, les dividendes et les dettes hypothécaires. Ce rapportage, qui n'est pas effectué en temps réel mais annuellement, est imposé à des fins de taxation et non de contrôle permanent.

Lors d'une troisième phase, des réformes ont été menées dans le cadre d'initiatives de l'Union européenne et de l'Organisation de coopération et de développement économiques (OCDE). La première loi nationale réglant le traitement des données à caractère personnel (*Personuppgiftslagen*) a ainsi été introduite en 1998, conformément à la directive européenne 95/46/CE qui était en vigueur à l'époque. Cette loi a ensuite servi de base à la loi suédoise portant exécution du Règlement général sur la protection des données (RGPD). Depuis 2010, la Suède a également intégré la norme commune de déclaration de l'OCDE et les directives européennes anti-blanchiment. Elle a aussi instauré un registre de comptes national (*Kontoregister*), géré exclusivement par les banques elles-mêmes et non par les autorités, dans lequel les banques ont l'obligation d'associer des numéros de compte à leurs titulaires.

L'autorité de contrôle financier suédoise (*Finansinspektionen* ou FI) veille au respect des obligations en matière de lutte contre le blanchiment et en rend compte à la cellule de renseignement financier (CRF) suédoise (*Finanspolisen*), qui est comparable à la Cellule de traitement des informations financières (CTIF) en Belgique. L'administration fiscale suédoise reçoit uniquement les données financières qui sont strictement nécessaires à la taxation, et ce, exclusivement dans le cadre de la loi sur les procédures fiscales (*Skatteförfarandelagen* ou SFL).

Depuis 2017, il existe aussi une loi nationale suédoise visant à lutter contre le blanchiment de capitaux et le financement du terrorisme (*Lag om åtgärder mot penningtvätt och finansiering av terrorism*), qui transpose les directives européennes 2015/849 et 2018/843. Cette loi ne contient pas non plus de dispositions autorisant le *data mining* par les autorités.

De heer Van Quickenborne overloopt vervolgens de verschillende juridische grondslagen van de Zweedse versie van een – gedecentraliseerd – CAP. De eerste grondslag is de voornoemde wet op de fiscale procedures, die de procedures voor belastingheffing, inning en informatieverplichting regelt. Hoofdstuk 40 van die wet, vergelijkbaar met artikel 322 van het Belgische Wetboek van de inkomstenbelastingen (WIB), omvat bepalingen over de informatie-uitwisseling met derden, waaronder banken. Zo mag de Zweedse belastingdienst enkel informatie opvragen in het kader van een concreet dossier of een specifieke belastingplicht, en zijn banken verplicht om hun medewerking te verlenen, zij het uitsluitend voor specifieke personen of entiteiten. De opgevraagde informatie moet noodzakelijk zijn voor de belastingheffing of -controle en mag niet worden hergebruikt voor andere doeleinden zonder nieuwe wettelijke basis. De overheid mag niet meer gegevens vragen dan strikt noodzakelijk. Er is dus geen structurele of algemene toegang tot bankgegevens, enkel een casuïstische bevraging.

De tweede juridische grondslag is het grondwettelijke principe van openbaarheid van bestuur, vastgelegd in hoofdstuk 2 van de persvrijheidswet, dat de administratie verplicht tot openheid en publieke controle. Paradoxaal genoeg versterkt dat principe ook de rechtsbescherming van individuen, aangezien elke overheidsverwerking openbaar kan worden getoetst. De Zweedse Raad van State (*Högsta förvaltningsdomstolen*) heeft geoordeeld dat openbaarheid impliceert dat er geen geheime gegevensverwerking kan plaatsvinden zonder wettelijke basis. Transparantie vormt dus de bescherming tegen willekeurige surveillance.

De derde juridische grondslag wordt gevormd door de *Kreditupplysningslag*, de wet op kredietinformatie van 1973, herzien in 2004. Die wet bepaalt dat commerciële kredietbureaus enkel gegevens mogen verwerken die relevant zijn voor kredietwaardigheid, en dit onder toezicht van de Zweedse gegevensbeschermingsautoriteit. Hoewel deze wet economisch van aard is, heeft zij ook gevolgen voor de fiscale context: banken mogen geen gegevens delen met de overheid, tenzij de wet op de fiscale procedures of de antiwitwaswet dit uitdrukkelijk toestaat.

De vierde juridische grondslag is de voormelde wet inzake maatregelen tegen het witwassen van geld en de financiering van terrorisme, die banken, makelaars en andere instellingen verplicht tot klantenidentificatie (volgens het principe *Know Your Customer*), transactie-monitoring en melding van verdachte activiteiten aan de

M. Van Quickenborne énumère ensuite les fondements juridiques de la version suédoise du PCC (décentralisé). La loi précitée sur les procédures fiscales, qui encadre les procédures d'imposition, de perception et d'obligation d'information, constitue le premier fondement. Le chapitre 40 de cette loi, comparable à l'article 322 du Code belge des impôts sur les revenus (CIR), contient des dispositions relatives à l'échange d'informations avec des tiers, notamment les banques. Ainsi, l'administration fiscale suédoise ne peut réclamer des informations que dans le cadre d'un dossier concret ou d'une obligation fiscale spécifique; les banques, quant à elles, sont tenues de coopérer pour autant que la demande d'informations porte sur des personnes ou des entités spécifiques. Les informations demandées doivent être nécessaires à des fins d'imposition ou de contrôle et ne peuvent être réutilisées à d'autres fins en l'absence de nouvelle base légale. Les autorités ne peuvent réclamer plus d'informations que ce qui est strictement nécessaire. Elles ne jouissent donc pas d'un accès structurel ou généralisé aux données bancaires et ne peuvent consulter celles-ci qu'au cas par cas.

Le deuxième fondement juridique est le principe constitutionnel de publicité de l'administration, inscrit dans le chapitre 2 de la loi sur la liberté de la presse. En vertu de ce principe, l'administration est tenue de faire preuve d'ouverture et de se soumettre à des contrôles publics. Paradoxalement, ce principe renforce également la protection juridique des individus, puisque tout traitement de données par les autorités peut être contrôlé publiquement. Selon le Conseil d'État suédois (*Högsta förvaltningsdomstolen*), la publicité de l'administration exclut tout traitement de données secret sans base légale. La transparence constitue donc une protection contre la surveillance arbitraire.

M. Van Quickenborne évoque ensuite le troisième fondement juridique, à savoir la loi sur les informations de crédit de 1973 (*Kreditupplysningslag*), révisée en 2004. Cette loi dispose que les agences de crédit commerciales ne peuvent traiter que les informations pertinentes pour la solvabilité, et ce, sous la supervision de l'autorité suédoise de protection des données. Bien que cette loi porte sur le volet économique, elle a également des répercussions fiscales: les banques ne peuvent pas partager de données avec les autorités, sauf si la loi sur les procédures fiscales ou la loi anti-blanchiment l'autorise expressément.

Le quatrième fondement juridique est la loi précitée sur les mesures de lutte contre le blanchiment d'argent et le financement du terrorisme, qui oblige les banques, les courtiers et autres établissements à identifier leurs clients (selon le principe *Know Your Customer*), à surveiller les transactions et à signaler toute activité suspecte

Zweedse financiële inlichtingeneenheid. Overeenkomstig deze antiwitwaswet mogen de verzamelde gegevens echter uitsluitend gebruikt worden voor de preventie van witwassen en terrorismefinanciering, en niet voor fiscale profilering.

De vijfde en laatste juridische grondslag wordt gevormd door de Zweedse wet van 2018 met aanvullende bepalingen bij de Europese AVG, waarmee de eerdere gegevensbeschermingswet van 1992 werd vervangen. De wet van 2018 bevat bepalingen inzake het inzagerecht, de verplichting tot dataminimalisatie en het verbod op geautomatiseerde besluitvorming zonder menselijke tussenkomst. Met de wet werden bovendien de bevoegdheden versterkt van de Zweedse gegevensbeschermingsautoriteit, de *Integritetsskyddsmyndigheten* (IMY), die onafhankelijk toezicht uitoefent.

Binnen het Zweedse systeem is de belastingdienst als centrale belastingautoriteit verantwoordelijk voor de belastingheffing en inning, de registratie van natuurlijke personen, het beheer van het nationale persoonsnummersysteem en de uitvoering van het bevolkingsregister. Hoewel de belastingdienst veel persoonsgegevens beheert, heeft zij geen directe of permanente toegang tot banktransacties. Banken leveren enkel de jaarlijkse *kontrolluppgifter* – gegevens over rente, leningen en dividenden – aan de overheid. Bij een vermoeden van fraude kan de Zweedse belastingdienst specifieke informatie opvragen, maar uitsluitend na schriftelijke motivering. Elk verzoek moet intern worden goedgekeurd door zowel een controleur als een afdelingshoofd.

De Zweedse financiële toezichthouder ziet toe op de naleving van de wetgeving inzake financiële diensten en antiwitwasregels. Zij beschikt over de bevoegdheid om administratieve sancties op te leggen aan banken die hun meldingsplicht of *Know Your Customer*-verplichtingen niet naleven. Zij heeft echter geen bevoegdheid om individuele klantgegevens te analyseren of te delen met andere overheden. Haar rol beperkt zich strikt tot het toezicht op de naleving van wettelijke verplichtingen en niet tot het gebruik van gegevens voor belastingdoeleinden.

De Zweedse financiële inlichtingeneenheid maakt deel uit van de Zweedse politie en ontvangt meldingen van verdachte transacties. De eenheid werkt samen met andere financiële inlichtingeneenheden, waaronder de Nederlandse FIU en de Belgische CFI. Zij kan transacties blokkeren of onderzoeken opstarten op grond van de antiwitwaswet, maar staat daarbij onder streng toezicht van het ministerie van Justitie en de Zweedse gegevensbeschermingsautoriteit. Geautomatiseerde

à la cellule suédoise de traitement des informations financières. Conformément à cette loi anti-blanchiment, les informations recueillies ne peuvent être utilisées qu'à des fins de prévention du blanchiment et du financement du terrorisme, et non en vue d'un profilage fiscal.

M. Van Quickenborne poursuit en évoquant le cinquième et dernier fondement, à savoir la loi suédoise de 2018 contenant des dispositions complémentaires au RGPD, qui a remplacé la précédente loi sur la protection des données de 1992. Cette loi de 2018 contient des dispositions relatives au droit d'accès, à l'obligation de minimisation des données et à l'interdiction de prise de décision automatisée sans intervention humaine. Elle a également renforcé les pouvoirs de l'autorité suédoise de protection des données (*Integritetsskyddsmyndigheten* (IMY)), qui exerce un contrôle indépendant.

Dans le système suédois, le fisc en tant qu'autorité fiscale centrale est responsable de la perception et du recouvrement des impôts, de l'enregistrement des personnes physiques, de la gestion du système national d'identification des personnes et de la tenue du registre de la population. Bien que l'administration fiscale gère de nombreuses données à caractère personnel, elle n'a pas d'accès direct ou permanent aux transactions bancaires. Les banques ne lui communiquent que les données annuelles relatives aux intérêts, aux prêts et aux dividendes (*kontrolluppgifter*). En cas de présomption de fraude, l'administration fiscale suédoise peut demander des informations spécifiques, mais uniquement après avoir motivé sa demande par écrit. Chaque demande doit être approuvée en interne à la fois par un contrôleur et par un chef de service.

L'autorité de contrôle prudentiel suédoise veille au respect de la législation relative aux services financiers et aux règles anti-blanchiment. Elle est habilitée à infliger des sanctions administratives aux banques qui ne respectent pas leur obligation de signalement ou leurs obligations en matière de *Know Your Customer*. Elle n'est toutefois pas habilitée à analyser les données individuelles des clients ni à les partager avec d'autres autorités. Son rôle se limite strictement au contrôle du respect des obligations légales et ne s'étend pas à l'utilisation des données à des fins fiscales.

L'unité suédoise de renseignement financier fait partie de la police suédoise et reçoit des signalements de transactions suspectes. Cette unité coopère avec d'autres cellules de renseignement financier, notamment la FIU néerlandaise et la CTIF belge. Elle peut bloquer des transactions ou ouvrir des enquêtes sur la base de la loi anti-blanchiment, mais elle est placée sous le contrôle strict du ministère de la Justice et de l'autorité suédoise de protection des données. La législation suédoise interdit

datamining is in Zweden wettelijk verboden. Analyses van financiële gegevens moeten steeds worden uitgevoerd door een menselijke analist.

De IMY, de Zweedse gegevensbeschermingsautoriteit, is belast met het toezicht op de naleving van de AVG en de nationale gegevensbeschermingswetgeving. Zij beschikt over ruime bevoegdheden. Zo kan zij audits uitvoeren bij overheden en banken, bindende bevelen uitvaardigen en administratieve geldboetes opleggen. In 2022 publiceerde de IMY een rapport waarin werd vastgesteld dat de Zweedse belastingdienst voldeed aan de eisen van proportionaliteit en doelbinding, en dat er geen aanwijzing was van systematisch gebruik van financiële gegevens voor profilering. Dat bevestigt dat het Zweedse model geen preventieve risicoselectie toepast, in tegenstelling tot wat er voorgesteld wordt in het kader van *money control*.

Wat de mechanismen voor informatie-uitwisseling en -toezicht in Zweden betreft, zijn er drie hoofdvormen. Ten eerste rapporteren banken en financiële instellingen jaarlijks gegevens over rente, leningen en dividenden aan de Zweedse belastingdienst. Deze bevatten gegevens over de identiteit van de rekeninghouder, het totale bedrag aan betaalde rente, ontvangen dividenden, hypothecaire schulden en, in beperkte mate, saldi. Het vertrouwen in de overheid is in Zweden bijzonder groot, waardoor dergelijke meldingen als vanzelfsprekend worden beschouwd. Sinds 2001 maakt het land gebruik van vooraf ingevulde belastingaangiften. De Zweedse belastingdienst gebruikt de ontvangen gegevens uitsluitend ter verificatie van vrijwillige aangiften, niet voor permanente analyse.

Een tweede mechanisme betreft de gerichte bevraging bij verdenking. De Zweedse belastingdienst kan bij een concreet vermoeden van fraude bijkomende informatie opvragen volgens de in de SFL-wet bepaalde procedures. Elk verzoek moet gebaseerd zijn op een wettelijke grondslag, schriftelijk worden gemotiveerd en vooraf worden goedgekeurd door een leidinggevende. De bevraging mag enkel betrekking hebben op de betrokken belastingplichtige. Banken zijn verplicht binnen tien dagen te antwoorden, maar mogen weigeren op een wettelijke basis. Bij betwisting kan de Zweedse belastingdienst de zaak voorleggen aan een *förvaltningsrätten*, d.i. een administratieve rechtbank, die een snelle toets uitvoert.

Ten derde participeert Zweden actief in internationale samenwerking. Het land neemt deel aan het *Common Reporting Standard*-systeem en aan de Europese informatie-uitwisseling in het kader van de antiwitwasrichtlijnen.

l'exploration automatisée de données. Les analyses des données financières doivent donc toujours être réalisées par un analyste humain.

L'autorité suédoise de protection des données IMY est chargée de veiller au respect du RGPD et de la législation nationale en matière de protection des données. Ses compétences sont étendues: elle peut par exemple effectuer des audits auprès d'autorités publiques et de banques, émettre des injonctions contraignantes et infliger des amendes administratives. En 2022, l'IMY a publié un rapport constatant que l'administration fiscale suédoise respectait les exigences de proportionnalité et de finalité, et que rien n'indiquait un usage systématique des données financières à des fins de profilage. Cela confirme que le modèle suédois n'applique pas de sélection préventive des risques, contrairement à ce qui est proposé dans le cadre de *money control*.

Les mécanismes d'échange et de contrôle de l'information en Suède peuvent être regroupés en trois catégories principales. Premièrement, les banques et les établissements financiers transmettent chaque année à l'administration fiscale suédoise des données relatives aux intérêts, aux prêts et aux dividendes, qui comprennent l'identité des titulaires des comptes concernés, le montant total des intérêts versés, les dividendes perçus, les dettes hypothécaires et, dans une mesure limitée, les soldes. En Suède, la confiance dans les autorités est particulièrement forte, de sorte que ces notifications sont considérées comme évidentes. Depuis 2001, le pays recourt à des déclarations fiscales préremplies. L'administration fiscale suédoise utilise uniquement les données communiquées pour vérifier les déclarations volontaires, et non pour réaliser des analyses permanentes.

Deuxièmement, l'intervenant évoque le mécanisme du questionnaire ciblé, au moyen duquel l'administration fiscale suédoise peut, lorsqu'il existe des soupçons concrets de fraude, demander des informations complémentaires conformément aux procédures prévues par la loi SFL. Chaque demande doit reposer sur une base légale, être motivée par écrit et être approuvée au préalable par un supérieur hiérarchique. Le questionnaire ne doit porter que sur le contribuable concerné. Les banques sont tenues d'y répondre dans un délai de dix jours, mais peuvent refuser de le faire en invoquant une disposition légale. En cas de contestation, l'administration fiscale suédoise peut soumettre l'affaire à un *förvaltningsrätten*, c'est-à-dire un tribunal administratif, qui procède à un examen rapide du dossier.

Troisièmement, la Suède participe activement à la coopération internationale. Le pays prend part au système *Common Reporting Standard* ainsi qu'au réseau européen d'échange d'informations mis en œuvre dans le cadre

De Zweedse belastingdienst ontvangt buitenlandse gegevens via de automatische gegevensuitwisseling, maar analyseert deze uitsluitend in het kader van concrete belastingplichtigen. De gegevens worden maximaal tien jaar bewaard en niet gedeeld met andere administraties zonder wettelijke toestemming.

De spreker stipt vervolgens de constitutionele verankering en de Europese context van het Zweedse model aan. De Zweedse grondwet bepaalt dat iedere persoon beschermd is tegen inmenging van de overheid in zijn persoonlijke levenssfeer, tenzij de wet anders bepaalt. Elke beperking van dit recht vereist een formele wet en een proportionaliteitsbeoordeling door de *Riksdag*, het Zweedse parlement. Deze grondwettelijke bepaling fungeert als directe rem op de uitbreiding van fiscale bevoegdheden.

Naast de Zweedse grondwet speelt ook de Europese rechtsorde een rol. Zweden past strikt de rechtspraak van het Hof van Justitie van de Europese Unie toe. De spreker acht het opvallend dat de Zweedse regering, na de Nederlandse toeslagenaffaire, bevestigde dat grootschalige profilering door de overheid onverenigbaar was met de Zweedse constitutionele traditie. In 2021 verwierp de Zweedse minister van Financiën daarnaast een voorstel tot centrale analyse van transactiedata, omdat dit in strijd was met artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) en met het proportionaliteitsbeginsel van de AVG.

Zweden beschikt daarnaast over vier onafhankelijke justitieombudsmannen (*Justitieombudsmän*), die door het parlement worden benoemd. Zij houden toezicht op de wettigheid van bestuurshandelingen en hebben de bevoegdheid om klachten over dataverwerking te onderzoeken en disciplinaire maatregelen te bevelen. In 2019 onderzocht de justitieombudsman een klacht tegen de Zweedse belastingdienst wegens het opvragen van bankgegevens zonder voldoende motivering. De ombudsman oordeelde dat de fiscus zijn bevoegdheden had overschreden en beval een interne herziening van de procedures. Dit voorval toont aan dat externe controle in Zweden daadwerkelijk functioneert.

De spreker vat samen dat het Zweedse model zich onderscheidt door de afwezigheid van centralisatie: er bestaat geen nationaal bankregister onder overheidstoezicht. Gegevensverwerking vereist steeds een formele wettelijke grondslag en een individuele motivering. Er is een duidelijk institutioneel evenwicht: het beheer van gegevens ligt bij de banken, het gebruik bij de Zweedse

des directives anti-blanchiment. L'administration fiscale suédoise reçoit des données provenant de l'étranger grâce à l'échange automatique d'informations, mais elle analyse exclusivement celles qui concernent des contribuables bien spécifiques. Les données sont conservées pour une durée maximale de dix ans et ne sont pas partagées avec d'autres administrations sans autorisation légale.

L'intervenant évoque ensuite l'ancrage constitutionnel et le contexte européen du modèle suédois. La Constitution suédoise dispose que toute personne est protégée contre l'ingérence de l'État dans sa vie privée, sauf si la loi en dispose autrement. Toute limitation de ce droit requiert une loi formelle et un contrôle de proportionnalité par le *Riksdag*, le parlement suédois. Cette disposition constitutionnelle agit comme un frein direct à l'extension des compétences fiscales.

Outre la Constitution suédoise, l'ordre juridique européen joue également un rôle. La Suède applique strictement la jurisprudence de la Cour de justice de l'Union européenne. Selon l'intervenant, il est significatif qu'après le scandale néerlandais des allocations familiales, le gouvernement suédois ait confirmé que le profilage à grande échelle par les pouvoirs publics était incompatible avec la tradition constitutionnelle suédoise. En 2021, le ministre suédois des Finances a en outre rejeté une proposition visant à prévoir une analyse centralisée des données de transaction, au motif que celle-ci contreviendrait à l'article 8 de la Convention européenne des droits de l'homme (CEDH) ainsi qu'au principe de proportionnalité consacré par le RGPD.

La Suède dispose en outre de quatre médiateurs de justice indépendants (*Justitieombudsmän*), qui sont nommés par le parlement. Ces derniers contrôlent la légalité des actes administratifs et sont habilités à examiner les plaintes relatives au traitement des données et à ordonner des mesures disciplinaires. En 2019, un médiateur de justice a ainsi examiné une plainte déposée à l'encontre de l'administration fiscale suédoise pour avoir réclamé des données bancaires sans justification suffisante. Le médiateur a estimé que le fisc avait outrepassé ses compétences et a ordonné une révision interne des procédures. Cet incident montre qu'en Suède, le contrôle externe fonctionne réellement.

En résumé, l'intervenant indique que le modèle suédois se démarque par son absence de centralisation: il n'existe pas de registre bancaire national placé sous le contrôle de l'autorité publique. Le traitement des données requiert toujours un fondement légal formel, ainsi qu'une motivation individuelle. Il existe un équilibre institutionnel manifeste: la gestion des données est du

belastingdienst en het toezicht bij de Zweedse gegevensbeschermingsautoriteit en de justitieombudsmannen. Daarnaast geldt functionele transparantie: overheidshandelingen zijn openbaar, maar private gegevens niet. Er is geen sprake van automatische selectie of profilering.

Zweden combineert aldus fiscale efficiëntie met constitutionele discipline. Het land bewijst dat openheid en privacy elkaar niet hoeven uit te sluiten, zolang de staat zichzelf juridisch begrenst. De vraag rijst echter of de Belgische federale regering over dezelfde discipline beschikt om die zelfbeperking te waarborgen en de staat tegen zichzelf te beschermen.

Het commissielid licht vervolgens toe hoe het Zweedse belastingmodel in de praktijk functioneert. Het Zweedse systeem steunt niet op een logica van preventieve controle, maar op het principe van verantwoord vertrouwen: burgers worden geacht correct te handelen, terwijl de overheid enkel controleert wanneer dat redelijk en gerechtvaardigd is. Dit mechanisme stelt de overheid in staat fiscale rechtvaardigheid te handhaven zonder daarbij de persoonlijke autonomie van de burger aan te tasten.

De heer Van Quickenborne verduidelijkt voorts eerst de praktische werking van het Zweedse belastingstelsel.

Er bestaat een jaarlijkse rapporteringscyclus waarbij banken hun controlerapporten overmaken aan de Zweedse belastingdienst. Die dienst verwerkt de gegevens om vooraf ingevulde belastingaangiften te genereren. Burgers ontvangen vervolgens een overzicht van hun inkomsten en aftrekposten dat zij enkel hoeven te bevestigen. Dit systeem kent een hoge naleving: 96 % van de aangiften wordt digitaal ingediend, met een foutenmarge van minder dan 1 %. Banken leveren dus gegevens aan, maar de overheid krijgt geen directe inzage in bankrekeningen.

Daarnaast licht het lid toe dat de Zweedse belastingdienst ad hoc bevestigingen kan uitvoeren bij een vermoeden van fraude. Wanneer vermoed wordt dat inkomsten onjuist zijn aangegeven, kan de Zweedse belastingdienst op basis van de wet op de fiscale procedures een schriftelijk informatieverzoek indienen bij een bank. Dit verzoek moet betrekking hebben op een duidelijk geïdentificeerde persoon of entiteit en er moet expliciet gemotiveerd worden waarom de gevraagde gegevens noodzakelijk zijn. De bank is verplicht te antwoorden, maar kan weigeren als het verzoek disproportioneel is. In dat geval kan de Zweedse belastingdienst een beslissing

ressort des banques, tandis que leur utilisation relève du fisc suédois et que leur contrôle incombe à l'autorité suédoise de protection des données. À cela s'ajoute une transparence fonctionnelle: les actes de l'autorité sont du domaine public, contrairement aux données privées. Il n'est pas question de sélection ni de profilage automatiques.

La Suède conjugue ainsi une efficacité fiscale avec une discipline constitutionnelle. Le pays prouve que la publicité et la vie privée ne doivent pas s'exclure mutuellement, tant que l'État observe les limites que lui impose la loi. La question est toutefois de savoir si le gouvernement fédéral belge dispose de semblable discipline pour garantir l'autolimitation et se protéger contre lui-même.

Le membre explique ensuite comment le modèle fiscal suédois fonctionne en pratique. Le système suédois ne repose pas sur une logique de contrôle préventif, mais sur le principe de la confiance responsable: les citoyens sont supposés agir correctement, tandis que les pouvoirs publics n'effectuent des contrôles que lorsque cela est raisonnable et justifié. Ce mécanisme permet aux pouvoirs publics de garantir l'équité fiscale sans porter atteinte à l'autonomie personnelle des citoyens.

M. Van Quickenborne commence par expliquer le fonctionnement pratique du système fiscal suédois.

Il existe un cycle de rapportage annuel dans le cadre duquel les banques transmettent leurs rapports de contrôle à l'administration fiscale suédoise. Celle-ci traite les données afin de générer des déclarations fiscales préremplies. Les citoyens reçoivent ensuite un aperçu de leurs revenus et de leurs postes de déduction, qu'ils n'ont plus qu'à confirmer. Ce système bénéficie d'un taux de conformité élevé: 96 % des déclarations sont soumises par voie électronique, avec une marge d'erreur inférieure à 1 %. Les banques fournissent donc des données, mais les pouvoirs publics n'ont pas directement accès aux comptes bancaires.

En outre, le membre explique que l'administration fiscale suédoise peut effectuer des enquêtes ponctuelles en cas de suspicion de fraude. Lorsqu'elle soupçonne que des revenus n'ont pas été déclarés correctement, l'administration fiscale suédoise peut, en vertu de la loi sur les procédures fiscales, adresser une demande d'informations écrite à une banque. Cette demande doit concerner une personne ou une entité clairement identifiée et doit motiver explicitement pourquoi les informations demandées sont nécessaires. La banque est tenue de répondre, mais peut refuser si la demande est disproportionnée. Dans ce cas, l'administration fiscale

tot vordering vragen bij de *Förvaltningsrätten*, d.i. de Zweedse administratieve rechtbank. De rechtspraak bevestigt dat dit geen routineprocedure mag worden. Zo oordeelde de rechtbank van Stockholm in 2017 dat een algemene screening van bankrekeningen zonder concrete aanwijzingen van belastingontduiking in strijd is met artikel 2, hoofdstuk 6 van de Zweedse Grondwet. Op die manier verankert Zweden het subsidiariteitsbeginsel, waarbij een strenge controle enkel is toegestaan wanneer lichtere controlemiddelen onvoldoende blijken.

Tot slot benadrukt het commissielid de beperkte samenwerking tussen de verschillende betrokken overheidsdiensten. De Zweedse belastingdienst kan bij verdenking van witwassen informatie ontvangen van de overheidsdienst voor Financiën en van de douane, maar de interne koppeling van gegevens blijft strikt beperkt. De belastingdienst heeft geen directe toegang tot politiedatabases en elke gegevensuitwisseling vereist een formele kennisgeving én een voorafgaande proportionaliteitsafweging.

Vervolgens bespreekt de heer Van Quickenborne de risicobeheersing en dataverwerking binnen de Zweedse belastingdienst en licht hierbij drie kernelementen toe.

Wat het intern risicomodel betreft, gebruikt de Zweedse belastingdienst geavanceerde risicomodellen om te bepalen welke belastingaangiften mogelijk fouten bevatten. Hierbij worden afwijkingen in inkomenspatronen, statistische inconsistenties en herhaalde fouten uit het verleden geanalyseerd. De analyse beperkt zich strikt tot fiscale gegevens en sluit banktransacties uit. De algoritmen mogen enkel persoonsgegevens gebruiken die rechtstreeks uit aangiften of uit wettelijk toegestane bronnen afkomstig zijn. Het gaat dus om een vorm van datamining, maar zonder gebruik van bankgegevens.

Ten tweede benadrukt het lid het belang van menselijke toetsing en verantwoordelijkheid in het Zweedse dataverwerkingsmodel. Elk algoritmisch signaal wordt beoordeeld door een menselijke controleur. Sinds 2021 geldt het principe dat geen enkel automatisch besluit mag worden genomen zonder menselijke goedkeuring. De controleur moet bovendien de reden voor de selectie en de inhoud van de beoordeling verplicht documenteren in het dossier. De verantwoordelijke ambtenaar blijft persoonlijk aansprakelijk voor fouten in de gegevensverwerking of voor het disproportioneel gebruik van algoritmen.

suédoise peut demander une décision de réquisition auprès du *Förvaltningsrätten*, le tribunal administratif suédois. La jurisprudence confirme que cela ne doit pas devenir une procédure de routine. Ainsi, en 2017, le tribunal de Stockholm a jugé qu'un contrôle général des comptes bancaires sans indices concrets de fraude fiscale était contraire à l'article 2, chapitre 6, de la Constitution suédoise. La Suède consacre ainsi le principe de subsidiarité, selon lequel un contrôle strict n'est autorisé que lorsque des moyens de contrôle moins contraignants s'avèrent insuffisants.

Enfin, le membre souligne que la coopération entre les différents services publics concernés est réduite. En cas de suspicion de blanchiment d'argent, l'administration fiscale suédoise peut recevoir des informations du service public des Finances et de la douane, mais le couplage interne des données reste strictement limité. L'administration fiscale n'a pas d'accès direct aux bases de données de la police et tout échange de données nécessite une notification formelle et une évaluation préalable de la proportionnalité.

M. Van Quickenborne aborde ensuite la gestion des risques et le traitement des données au sein de l'administration fiscale suédoise, en mettant en avant trois éléments clés.

En ce qui concerne le modèle de risque interne, l'administration fiscale suédoise utilise des modèles de risque avancés pour déterminer quelles déclarations fiscales peuvent contenir des erreurs. Pour ce faire, elle analyse les anomalies dans les modèles de revenus, les incohérences statistiques et les erreurs répétées dans le passé. L'analyse se limite strictement aux données fiscales et exclut les transactions bancaires. Les algorithmes peuvent uniquement utiliser des données à caractère personnel provenant directement de déclarations ou de sources autorisées par la loi. Il s'agit donc d'une forme de *data mining*, mais sans utilisation de données bancaires.

Deuxièmement, le membre souligne l'importance du contrôle humain et de la responsabilité dans le modèle suédois de traitement des données. Chaque signal algorithmique est évalué par un contrôleur humain. Le principe selon lequel aucune décision automatique ne peut être prise sans approbation humaine est d'application depuis 2021. Le contrôleur est en outre tenu de documenter dans le dossier la raison de la sélection et le contenu de l'évaluation. Le fonctionnaire responsable assume personnellement la responsabilité des erreurs dans le traitement des données ou de l'utilisation disproportionnée des algorithmes.

Als derde punt gaat het commissielid in op de beperkingen van datamining. De Zweedse wetgeving biedt geen preventieve basis voor grootschalige datamining door de fiscus. Het gebruik van big data of machine learning om potentiële fraudeurs te identificeren is uitdrukkelijk verboden. De Zweedse gegevensbeschermingsautoriteit bevestigt in haar rapport van 2022 dat zelfs datasets voor beleidsanalyse eerst worden geanonimiseerd, waarbij alle identificeerbare elementen worden verwijderd. Bovendien worden gegevens niet samengevoegd uit verschillende domeinen, wat het risico op machtsconcentratie voorkomt en de bescherming van de persoonlijke levenssfeer versterkt.

De heer Van Quickenborne bespreekt vervolgens de rechtsbescherming voor burgers binnen het Zweedse belastingstelsel en licht drie belangrijke waarborgen toe.

Zweedse burgers hebben het recht om hun fiscale dossiers in te zien. De minister van Financiën, de heer Jan Jambon, verklaarde echter dat de zogenoemde DAM-fiches, de kern van de algoritmen, geen deel uitmaken van de dossiers in België. Hierdoor rijst volgens de heer Van Quickenborne de vraag hoe Belgische burgers zich effectief kunnen verdedigen wanneer zij de essentie van hun dossier niet mogen inzien. De omzetting van artikel 15 van de GDPR verleent burgers formeel recht op inzage in hun fiscaal dossier.

In Zweden worden betrokkenen bovendien na afloop van een bankbevraging door de belastingdienst geïnformeerd over welke gegevens zijn opgevraagd, bij welke bank en op basis van welke wettelijke grondslag. In België daarentegen ontvangen burgers die informatie niet automatisch; zij moeten die zelf opvragen, hetzij via een schriftelijke procedure bij de Nationale Bank, hetzij digitaal. In Zweden kan de kennisgeving tijdelijk worden uitgesteld om lopende onderzoeken niet te hinderen, maar zij moet plaatsvinden zodra het dossier is afgesloten. In de praktijk ontvangt de burger binnen dertig dagen een melding.

Ten tweede, bespreekt het commissielid de mogelijkheid die bestaat in Zweden om een bezwaar in te dienen tegen de gegevensverwerking door de Zweedse belastingdienst. Indien het bezwaar van een burger wordt afgewezen, kan er beroep worden aangetekend bij de rechtbank. De rechter toetst daarbij de proportionaliteit, de noodzakelijkheid van het gegevensgebruik en de procedurele correctheid van het informatieverzoek. De Zweedse rechtspraak is op dit punt streng: in 2019 vernietigde de rechtbank een verzoek van de fiscus dat te algemeen was geformuleerd en geen concrete aanwijzingen van fraude bevatte.

Le membre aborde ensuite les limites du *data mining*. La législation suédoise n'offre aucune base préventive pour un *data mining* à grande échelle par le fisc. L'utilisation des mégadonnées ou de l'apprentissage automatique (*machine learning*) pour identifier les fraudeurs potentiels est expressément interdite. Dans son rapport de 2022, l'Autorité de protection des données suédoise confirme que même les ensembles de données destinés à l'analyse politique sont d'abord anonymisés, tous les éléments identifiables étant supprimés. En outre, les données provenant de différents domaines ne sont pas fusionnées, ce qui évite le risque de concentration du pouvoir et renforce la protection de la vie privée.

M. Van Quickenborne aborde ensuite la question de la protection juridique des citoyens dans le cadre du système fiscal suédois et commente trois garanties importantes.

Les citoyens suédois ont le droit de consulter leurs dossiers fiscaux. M. Jan Jambon, ministre des Finances, a toutefois déclaré que les "fiches DAM", qui constituent le cœur des algorithmes, ne font pas partie des dossiers en Belgique. Selon M. Van Quickenborne, cela soulève la question de savoir comment les citoyens belges pourront se défendre efficacement s'ils ne sont pas autorisés à consulter l'essentiel de leurs dossiers respectifs. La transposition de l'article 15 du RGPD confère à tout citoyen un droit d'accès formel à son dossier fiscal.

En Suède, les personnes concernées sont également informées, après toute enquête bancaire menée par l'administration fiscale, des données qui ont été demandées, de la banque visée et de la base légale invoquée. En Belgique, en revanche, les citoyens ne reçoivent pas ces informations automatiquement mais doivent les demander eux-mêmes, soit par écrit à la Banque nationale, soit par voie électronique. En Suède, la notification peut être temporairement reportée pour ne pas entraver une enquête en cours, mais elle doit avoir lieu dès que le dossier est clos. En pratique, le citoyen est informé dans un délai de trente jours.

Deuxièmement, l'intervenant évoque la possibilité, prévue en Suède, d'introduire une réclamation contre le traitement des données par l'administration fiscale suédoise. Lorsque la réclamation d'un citoyen est rejetée, il peut introduire un recours devant le tribunal. Le juge examine alors la proportionnalité, la nécessité de l'utilisation des données et la conformité procédurale de la demande d'informations. La jurisprudence suédoise est stricte en la matière: en 2019, le tribunal a annulé une demande de l'administration fiscale qui était formulée de manière trop générale et ne contenait aucun indice concret de fraude.

Ten derde, wijst het lid op het recht van de Zweedse burger op het indienen van een klacht en het eisen van een schadevergoeding. De Zweedse gegevensbeschermingsautoriteit behandelt klachten over onrechtmatige gegevensverwerking en kan zowel de verwijdering van gegevens bevelen als boetes opleggen aan de overheid. Daarnaast kan de burger een schadevergoeding eisen op grond van artikel 82 van de GDPR of artikel 3 van de Zweedse aansprakelijkheidswet. De justitieombudsmannen beschikken bovendien over de bevoegdheid om tuchtrechtelijke maatregelen te nemen tegen ambtenaren die de wet overtreden. Deze meervoudige structuur van toezicht en herstelmechanismen maakt van Zweden een van de meest verantwoordelijke bestuursmodellen van Europa.

De heer Van Quickenborne staat voorts stil bij de toezichtmechanismen in Zweden en benadrukt dat deze een evenwicht zoeken tussen efficiënt bestuur en bescherming van de persoonlijke levenssfeer.

Ten eerste wijst de spreker op de rol van de Zweedse gegevensbeschermingsautoriteit, die jaarlijks audits uitvoert bij overheidsdiensten. In 2022 onderzocht de autoriteit de Zweedse belastingdienst en concludeerde dat de procedurele controles voldoen aan de vereisten van de GDPR. De administratie informeert burgers sneller en archiveert de motiveringen nauwkeuriger bij bankbevragingen. De Zweedse gegevensbeschermingsautoriteit publiceert bovendien richtlijnen over het verbod op geautomatiseerde besluitvorming en over de verplichte Digital Process Impact Assessments (DPIA's) bij het gebruik van algoritmen.

Daarnaast is er sprake van een parlementair toezicht. Het Zweedse parlement ontvangt jaarlijks het integriteitsrapport van de overheidsdienst Financiën. De commissie voor de Grondwet en Openbaar Bestuur van het Zweedse parlement behandelt klachten over privacyschendingen door de overheid. De debatten over dataverwerking verlopen openbaar en transparant en worden live uitgezonden, vergelijkbaar met de praktijk in België.

Verder controleert de Zweedse Rekenkamer de efficiëntie en wettelijkheid van administratieve processen. In haar verslag van 2021 stelde zij vast dat het Zweedse belastinginformatiesysteem voldoet aan de hoge eisen van proportionaliteit en dat de balans tussen efficiëntie en privacy behouden blijft.

Tot slot stelt de heer Van Quickenborne dat Zweden een sterke cultuur van vertrouwen kent met een hoge fiscale moraliteit. De bereidheid tot aangifte en betaling geldt er

Troisièmement, le membre souligne le droit reconnu au citoyen suédois d'introduire une plainte et de demander réparation. L'autorité suédoise de protection des données suédoise traite les plaintes relatives à tout traitement illicite de données et peut à la fois ordonner la suppression de ces données et infliger des amendes à l'administration. Par ailleurs, le citoyen peut réclamer réparation en vertu de l'article 82 du RGPD ou de l'article 3 de la loi suédoise sur la responsabilité civile. L'ombudsman de la justice est en outre habilité à prendre des mesures disciplinaires contre les fonctionnaires qui enfreignent la loi. Cette structure multiple de contrôle et de mécanismes de réparation fait de la Suède l'un des modèles de gouvernance les plus responsables d'Europe.

M. Van Quickenborne aborde ensuite la question des mécanismes de contrôle en vigueur en Suède et souligne que ceux-ci visent à trouver un équilibre entre une administration efficace et la protection de la vie privée.

Premièrement, l'intervenant rappelle le rôle de l'Autorité suédoise de protection des données, qui réalise chaque année des audits auprès des services publics. En 2022, cette autorité a conclu, après avoir audité l'administration fiscale suédoise, que ses contrôles procéduraux répondaient aux exigences du RGPD. L'administration informe les citoyens plus rapidement, et archive plus rigoureusement les motifs des demandes adressées aux banques. L'Autorité suédoise de protection des données publie en outre des lignes directrices sur l'interdiction de la prise de décision automatisée et sur l'obligation de réaliser des évaluations d'impact des processus numériques (*Digital Process Impact Assessments*, DPIA) lors de l'utilisation d'algorithmes.

À cela s'ajoute un contrôle parlementaire. Le Parlement suédois reçoit chaque année le rapport d'intégrité du service public des Finances. La commission de la Constitution et de l'administration du Parlement suédois traite les plaintes relatives aux violations de la vie privée commises par les autorités publiques. Les débats sur le traitement des données sont publics et transparents, et ils sont diffusés en direct, comme en Belgique.

En outre, la Cour des comptes suédoise contrôle l'efficacité et la légalité des processus administratifs. Dans son rapport de 2021, elle constate que le système d'information fiscale suédois satisfait aux exigences élevées de proportionnalité et que l'équilibre entre efficacité et protection de la vie privée est préservé.

Enfin, M. Van Quickenborne souligne qu'en Suède, la culture de confiance est forte et la moralité fiscale est grande. La disposition à déclarer ses revenus et

als een gedeelde maatschappelijke norm. De Zweedse belastingdienst publiceert regelmatig rapporten over ethiek en vertrouwen, waarbij transparantie wordt beschouwd als de basis voor naleving. Controle zonder vertrouwen is repressie; vertrouwen zonder controle is naïviteit.

De heer Lode Vereeck (VB) verwijst naar eerder onderzoek over verkeersveiligheid, waarin werd vastgesteld dat landen met sterk uiteenlopende verkeerswetgevingen toch vergelijkbare lage aantallen verkeersongevallen kunnen hebben. Volgens de spreker ligt de verklaring in wat men noemt rechtsgetrouwheid of de bereidheid van burgers om de regels na te leven.

De heer Vereeck merkt op dat in landen zoals Zweden deze maatschappelijke bereidheid om de regels te volgen aanzienlijk groter is dan in andere landen. Dit fenomeen is meetbaar via de corruptie-index, die volgens hem in wezen een rechtsgetrouwheidsindex weerspiegelt. Zweden scoort daar bijzonder hoog op.

De spreker benadrukt dat deze rechtsgetrouwheid zich niet enkel manifesteert in het verkeersrecht, maar ook in andere domeinen zoals de fiscaliteit. Hij suggereert dat deze houding, volgens bepaalde sociaalwetenschappelijke onderzoekers, mogelijk verband houdt met het protestantse karakter van landen zoals Zweden, het Verenigd Koninkrijk en Nederland, waar discipline en plichtsbesef diep verankerd zijn. De Zweedse overheid zou zich hierdoor kunnen permitteren om een hoge mate van vertrouwen te schenken aan haar burgers, omdat deze laatste effectief bereid zijn om de gezamenlijk vastgelegde regels te volgen. In landen waar die rechtsgetrouwheid minder aanwezig is, besluit de heer Vereeck, zal men wellicht tot een andere bestuurlijke aanpak moeten komen.

De heer Vincent Van Quickenborne (Open Vld) benadrukt dat het de taak van de overheid is om een cultuur van vertrouwen te bevorderen, zodat burgers op hun beurt ook vertrouwen in de overheid kunnen hebben. Volgens de spreker ondermijnt een streng geldcontrolesysteem dit principe, aangezien het uitgaat van het vermoeden dat alle burgers potentiële fraudeurs zijn. In zo'n context is het volgens het commissielid begrijpelijk dat burgers hun vertrouwen in de overheid verliezen. Ook de belastingssystemen in Duitsland, Oostenrijk, Nederland, Zweden en Finland, landen die vaak beïnvloed zijn door een protestantse cultuur van verantwoordelijkheid en zelfdiscipline, illustreren dat vertrouwen een sterkere volgzzaamheid bevordert. Volgens het commissielid zouden deze voorbeelden ook België moeten inspireren.

à payer ses impôts y est perçue comme une norme sociale partagée. L'administration fiscale suédoise publie régulièrement des rapports sur l'éthique et la confiance dans lesquels la transparence est considérée comme le fondement du respect des règles. Le contrôle sans confiance est une forme de répression tandis que la confiance sans contrôle est une forme de naïveté.

M. Lode Vereeck (VB) évoque une étude sur la sécurité routière réalisée par le passé, qui a révélé que des pays appliquant des législations très différentes en matière de circulation routière parvenaient malgré tout à obtenir un niveau similaire et faible d'accidents de la route. Selon l'intervenant, l'explication réside dans la "fidélité au droit" ou la volonté des citoyens de se conformer aux règles.

M. Vereeck fait observer que dans des pays comme la Suède, les citoyens sont bien plus disposés à respecter les règles que dans d'autres pays. Ce phénomène peut être mesuré à l'aide de l'indice de la corruption, qui, selon l'intervenant, équivaut en soi à un indice de la fidélité au droit. La Suède obtient un score particulièrement élevé dans ce domaine.

L'intervenant souligne que cette fidélité au droit ne se manifeste pas seulement dans la législation en matière de roulage, mais également dans d'autres domaines tels que la fiscalité. Il suggère que cette attitude, selon certains chercheurs en sciences sociales, pourrait être liée au caractère protestant de pays tels que la Suède, le Royaume-Uni et les Pays-Bas, où la discipline et le sens du devoir sont profondément ancrés. Les autorités suédoises pourraient ainsi se permettre d'accorder une grande confiance à leurs citoyens, car ces derniers sont réellement disposés à respecter les règles fixées collectivement. M. Vereeck conclut en indiquant que les pays moins marqués par cette fidélité au droit devraient peut-être adopter une autre approche administrative.

M. Vincent Van Quickenborne (Open Vld) souligne qu'il incombe aux pouvoirs publics de promouvoir une culture de confiance afin que les citoyens puissent à leur tour avoir toute confiance dans les pouvoirs publics. Selon l'intervenant, un système de contrôle financier sévère compromettra ce principe, car il part du postulat que tous les citoyens sont des fraudeurs potentiels. Dans ce contexte, il est compréhensible, selon l'intervenant, que les citoyens perdent confiance dans les pouvoirs publics. Les systèmes fiscaux de l'Allemagne, de l'Autriche, des Pays-Bas, de la Suède et de la Finlande, pays souvent influencés par une culture protestante marquée par la responsabilité et l'autodiscipline, illustrent également que la confiance favorise une plus grande docilité. Selon le membre, la Belgique devrait aussi s'inspirer de ces exemples.

De heer Van Quickenborne waarschuwt dat het voorliggende wetsontwerp een gevaarlijk precedent kan scheppen. Zonder duidelijke grenzen of controlemechanismen bestaat het risico dat de macht van de fiscus te ver reikt.

De spreker benadrukt dat er in Zweden geen aanwijzingen zijn van misbruik of datalekken. De Zweedse gegevensbeschermingsautoriteit publiceert jaarlijks rapporten over datalekken in de publieke sector. In de periode 2018 tot 2023 werden geen noemenswaardige incidenten vastgesteld bij de Zweedse belastingdienst inzake financiële gegevens. Dit contrasteert scherp met andere Europese landen waar centralisatie de kwetsbaarheid inzake datalekken net heeft vergroot.

De heer Van Quickenborne vergelijkt vervolgens de situatie in Zweden met die in België.

In Zweden wordt het beheer van financiële data toevertrouwd aan de banken, terwijl dit in België gebeurt door de Nationale Bank. Zweden beschikt niet over een centraal register, in tegenstelling tot België, waar dit wel bestaat.

Wat profilering betreft, is deze praktijk in Zweden verboden, terwijl ze in België wordt toegestaan onder het nieuwe wetsontwerp. De toegang van de overheid tot financiële gegevens gebeurt in Zweden enkel op gemotiveerd verzoek, terwijl die in België permanent en automatisch zou worden.

Ook op het vlak van transparantie naar de burger bestaan er duidelijke verschillen. In Zweden is een kennisgeving aan de betrokkene verplicht na afloop van een onderzoek, terwijl in een dergelijke verplichting in België niet is voorzien.

Wat het toezicht betreft, beschikt in Zweden de gegevensbeschermingsautoriteit, de justitieombudsmannen en het Parlement over deze bevoegdheid, terwijl in België enkel de Gegevensbeschermingsautoriteit (GBA) toezicht uitoefent met beperkte bevoegdheden. Daarnaast is er in Zweden een duidelijke functionele scheiding tussen het beheer, het gebruik en het toezicht op financiële data. In België daarentegen zijn al deze verantwoordelijkheden geconcentreerd bij de FOD Financiën.

Tot slot wijst het lid op het verschil in bestuurscultuur: Zweden wordt gekenmerkt door openheid en een hoog vertrouwen van de burger, terwijl België nog steeds kampt met een cultuur van administratieve geslotenheid.

M. Van Quickenborne met en garde contre le fait que le projet de loi à l'examen pourrait créer un dangereux précédent. En l'absence de limites et de mécanismes de contrôle clairs, un trop grand pouvoir pourrait être concentré dans les mains de l'administration fiscale.

L'intervenant souligne qu'il n'existe en Suède aucune indication d'abus ou de fuites de données. L'Autorité de protection des données suédoise publie chaque année des rapports sur les fuites de données dans le secteur public. Entre 2018 et 2023, aucun incident notable n'a été constaté au sein de l'administration fiscale suédoise en ce qui concerne les données financières. Cette situation contraste fortement avec celle d'autres pays européens où la centralisation a justement accru la vulnérabilité aux fuites de données.

M. Van Quickenborne compare ensuite la situation de la Suède à celle de la Belgique.

En Suède, la gestion des données financières est confiée aux banques, tandis qu'en Belgique, elle est assurée par la Banque nationale. Par ailleurs, notre pays dispose d'un registre central, ce qui n'est pas le cas de la Suède.

En ce qui concerne le profilage, cette pratique est interdite en Suède, alors que le nouveau projet de loi l'autorisera en Belgique. En Suède, les autorités publiques ne peuvent accéder aux données financières qu'en introduisant une demande motivée, alors qu'en Belgique, cet accès deviendrait permanent et automatique.

Il existe également des différences notables en matière de transparence à l'égard des citoyens. En Suède, une notification à la personne concernée est obligatoire à l'issue d'une enquête, alors que cette obligation n'est pas prévue en Belgique.

En ce qui concerne le contrôle, l'intervenant indique qu'en Suède, l'Autorité de protection des données, les médiateurs de justice et le Parlement disposent de cette compétence, tandis qu'en Belgique, seule l'Autorité de protection des données (APD) exerce un contrôle avec des compétences limitées. En outre, il existe en Suède une séparation fonctionnelle claire entre la gestion, l'utilisation et la surveillance des données financières. En Belgique, toutes ces responsabilités sont, en revanche, concentrées au sein du SPF Finances.

Enfin, l'intervenant souligne la différence de culture administrative: la Suède se caractérise par son ouverture et par une grande confiance accordée par les citoyens, tandis que la Belgique est toujours confrontée à une culture d'opacité administrative.

Volgens de heer Van Quickenborne toont deze vergelijking aan dat Zweden structureel meer vertrouwen stelt in zijn burgers en in het recht, terwijl België vertrekt vanuit een logica van preventieve controle. In Zweden is de overheid open over haar werking, maar terughoudend met persoonsgegevens; in België is het omgekeerd. Dat verschil is niet technisch, aldus de spreker, maar normatief en weerspiegelt een fundamenteel ander idee van staatsmacht.

Tot slot wijst het commissielid op de drievoudige verankering van de proportionaliteitstoets in Zweden: in de Grondwet, in de nationale toepassing van de GDPR en in de rechtspraak van het Hooggerechtshof. Elke inmenging moet volgens deze toets bij wet zijn voorzien, noodzakelijk voor een legitiem doel en evenredig zijn met dat doel. Het geplande Belgische systeem van *money control*, besluit de spreker, zal die proportionaliteitstoets niet doorstaan: het mist individuele noodzaak, werkt op algemene basis en schendt het evenredigheidsbeginsel.

5. Vergadering van 18 november 2025

De heer Vincent Van Quickenborne (*Open Vld*) herinnert eraan dat talrijke collega's hebben aangegeven het woord te willen nemen over deze belangrijke kwestie en dat de heer David Hatwick, onderzoeker aan de Universiteit Antwerpen, op maandag 24 november 2025 zijn doctoraat over dit onderwerp zal voorstellen, met als titel *Deus Tax Machina*.

Hij betreurt dat het debat over dit fundamentele onderwerp, namelijk het respect voor de privacy en de grondrechten, uitsluitend door de oppositie moet worden gevoerd.

De spreker hekelt de onjuiste beweringen van de heer Tas in een artikel dat op 15 november 2025 in *Het Nieuwsblad* verscheen (*Open Vld gooit alles in de strijd om nieuw wetsontwerp tegen te houden: "Deze overheid wantrouwt haar eigen burgers"*), waarin gesteld wordt dat het voorliggende wetsontwerp alleen betrekking zou hebben op georganiseerde fraude, terwijl de minister iets anders zegt.

Het lid betreurt het relatieve stilzwijgen in de pers en het gebrek aan debat in de publieke opinie, hoewel hij wel opmerkt dat het onderwerp stilaan begint te leven en er hier en daar artikelen over beginnen te verschijnen. Hij citeert het artikel dat op 18 november 2025 in *De Morgen* verscheen (*De fiscus wil slimme software loslaten op uw bankrekening in de strijd tegen fraude. Dit moet u weten over "money control"*).

Selon M. Van Quickenborne, il ressort de cette comparaison que la Suède accorde structurellement plus de confiance à ses citoyens et au droit, tandis que la Belgique s'appuie sur une logique de contrôle préventif. En Suède, les pouvoirs publics sont transparents quant à leur fonctionnement, mais prudents en matière de données à caractère personnel; en Belgique, c'est l'inverse. Selon l'intervenant, cette différence n'est pas technique, mais normative et reflète une conception fondamentalement différente du pouvoir de l'État.

Enfin, l'intervenant souligne le triple ancrage du contrôle de proportionnalité en Suède: dans la Constitution, dans l'application nationale du RGPD et dans la jurisprudence de la Cour suprême. Dans le cadre de ce contrôle, toute ingérence doit être prévue par la loi, être nécessaire à la poursuite d'un objectif légitime et être proportionnée à cet objectif. L'intervenant conclut en indiquant que le système belge envisagé de *money control* ne satisfera pas à ce critère de proportionnalité: il ne répond pas à un besoin individuel, s'appuie sur une base générale et viole le principe de proportionnalité.

5. Réunion du 18 novembre 2025

M. Vincent Van Quickenborne (*Open Vld*) rappelle que de nombreux collègues ont exprimé le souhait de prendre la parole sur cette importante thématique et que M. David Hatwick, *PhD researcher* à l'Université d'Anvers, présentera lundi 24 novembre 2025 sa thèse de doctorat sur ce sujet avec comme titre *Deus Tax Machina*.

Il regrette que ce soit l'opposition seule qui doive mener le débat et la contradiction sur ce sujet fondamental pour le respect de la vie privée et des droits fondamentaux.

Il dénonce les mensonges proférés par M. Tas dans un article paru dans *Het Nieuwsblad* le 15 novembre 2025 (*Open Vld gooit alles in de strijd om nieuw wetsontwerp tegen te houden: "Deze overheid wantrouwt haar eigen burgers"*), arguant que le texte ne porterait que sur la fraude organisée alors que le ministre ne dit pas cela.

Le membre regrette le silence relatif dans la presse et le peu de débat dans l'opinion publique, même s'il observe un frémissement avec ça et là des articles qui commencent à fleurir sur le sujet. Il cite l'article paru dans *De Morgen* le 18 novembre 2025 (*De fiscus wil slimme software loslaten op uw bankrekening in de strijd tegen fraude. Dit moet u weten over "money control"*).

De spreker verwijst voorts naar het begraven van het project *chat control* onder druk van de publieke opinie en bepaalde fracties. Onder het Deense EU-voorzitterschap zou er echter een tweede versie in voorbereiding zijn, die via een omweg opnieuw op tafel zou komen.

De heer Lode Vereeck (VB) wil de minister ervan overtuigen met *money control* niet te doen wat men van plan was met *chat control* en waar men wegens respect voor de privacy en de grondrechten mee is opgehouden. Sommigen argumenteren dat *money control* in werkelijkheid slechts een instrument is voor de bestrijding van georganiseerde fraude, dat uitsluitend wordt gebruikt voor risicodetectie (*tax or fraud risk behavior*). *Money control* is echter al lang niet meer gericht op fraude, maar op de controle van alle aspecten van fiscaal gedrag, dus niet alleen de economische, maar ook de sociaalpsychologische aspecten.

De heer Vincent Van Quickenborne (Open Vld) voegt eraan toe dat het onderwerp nog verder reikt en betrekking heeft op het beginsel van tegenspraak en de keuze voor de minst belaste fiscale werkwijze, wat eenieders volste recht is en niets met fraude te maken heeft. Datamining houdt het grote risico in dat men aan profilering doet en zich baseert op oppervlakkige veronderstellingen.

Het lid herinnert aan zijn opmerking over het ontbreken van de adviezen van drie instanties: de KBO, de Inspectie van Financiën en de NBB. Voorts is hij teruggekomen op de twee belangrijke wetten inzake het CAP, namelijk die van 14 april 2011 en die van 8 juli 2018, alsook op de koninklijke uitvoeringsbesluiten. Hij heeft ook verwezen naar het evaluatiekader, inclusief de rol van de Commissie voor de bescherming van de persoonlijke levenssfeer, de latere Gegevensbeschermingsautoriteit (GBA). De spreker is ook teruggekomen op de basisteksten: de Belgische Grondwet (art. 22), de Europese teksten met artikel 22 van de AVG, artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en het Europees Sociaal Handvest. Tot slot werd ook de jurisprudentie van het Grondwettelijk Hof en die van het Hof van Justitie van de Europese Unie besproken.

Vervolgens heeft de heer Van Quickenborne een vergelijkende rechtsanalyse uitgevoerd met de Nederlandse, Duitse, Oostenrijkse, Zweedse en Finse modellen. Hij voegt eraan toe dat er inspiratie kan worden geput uit de praktijken in Ierland, het Groothertogdom Luxemburg en Zwitserland.

Hij betreurt dat het problematische gedeelte van de tekst via amendementen werd ingediend en niet meer dan zeven leden beslaat, die geenszins rekening houden met de adviezen van de Raad van State en de GBA. Hij

Il évoque ensuite l'enterrement du projet *chat control* à la suite de la pression de l'opinion publique et de certains groupes politiques. Cependant une version n° 2, sous la présidence danoise de l'Union européenne, serait en préparation et reviendrait sur la table d'une manière détournée.

M. Lode Vereeck (VB) souhaite convaincre le ministre de ne pas faire avec *money control* ce qui était prévu dans *chat control* et qui a été abandonné pour les raisons de respect de la vie privée et des droits fondamentaux. Certains avancent l'argument que *money control* ne serait en réalité qu'un outil pour lutter contre la fraude organisée mais uniquement utilisée à des fins de détection des risques ("*tax or fraud risk behavior*"). *Money control* n'est depuis longtemps déjà plus focalisé sur la fraude mais porte sur le contrôle de tous les aspects des comportements fiscaux, pas seulement économiques mais aussi socio-psychologiques.

M. Vincent Van Quickenborne (Open Vld) ajoute que le sujet va encore plus loin et porte sur le principe du contradictoire et le choix de la voix fiscale la moins imposée, ce qui est le droit le plus strict de chacun et n'a rien de frauduleux. Le risque de profilage et de se fier aux apparences est important à cause de l'exploration de données (*data mining*).

Le membre rappelle avoir mentionné l'absence d'avis de trois instances: la BCE, l'Inspection des finances et la BNB. Il est ensuite revenu sur les deux lois importantes sur le PCC, celles du 14 avril 2011 et du 8 juillet 2018, ainsi que les arrêtés royaux d'exécution. Il a également évoqué le cadre d'évaluation, avec le rôle de la commission pour le respect de la vie privée devenue ensuite l'autorité de protection des données (APD). Il est aussi revenu sur les textes fondamentaux: la Constitution belge (art. 22), les textes européens avec l'article 22 du RGPD, l'article 8 de la Convention européenne des droits de l'homme et la Charte sociale européenne. Enfin, la jurisprudence de la Cour constitutionnelle et celle de la CJUE.

Il s'est ensuite livré à un exercice de droit comparé avec les modèles néerlandais, allemand, autrichien, suédois et finlandais. Il ajoute qu'il y a lieu de s'inspirer des pratiques en cours en Irlande, au Grand-Duché de Luxembourg et en Suisse.

Il déplore que la partie du texte qui pose problème ait été introduite par le biais d'amendements et concerne en tout et pour tout sept alinéas, qui ne tiennent nullement compte des avis du Conseil d'État et de l'APD. Il ajoute

voegt eraan toe dat het toepassingsgebied werd uitgebreid tot cryptomunten en effectenrekeningen.

In het betoog dat volgt, zal hij terugkomen op de jurisprudentie van het Hof van Justitie van de Europese Unie (de arresten *Dun & Bradstreet* (C-203/22) en *Schuffa Holding* (C-634/21) van 7 december 2023) en de impact van artificiële intelligentie op de fiscaliteit, onder meer het schandaal rond de kinderbijslag in Nederland ('toeslagenaffaire'). Ook de *E-kasa* in Slowakije zal aan bod komen. Dat systeem van elektronische zelfregistrerende kassa's verplicht bedrijven die cash- of elektronische betalingen accepteren om zich aan te melden op de portalen van de Slowaakse belastingdienst. Het in juli 2019 ingevoerde systeem moet fiscale fraude bestrijden door middel van een gedetailleerde online monitoring van de transacties. Het systeem werd door het Slowaakse Grondwettelijk Hof nietig verklaard.

Hij zal vervolgens zijn licht werpen op de AI-Act van de Europese Unie (Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie).

Daarna wordt het tijd om de werking van *money control* en de drie pijlers ervan, namelijk datamining, SAQ-software en de DAM-fiches (*Digital Asset Management*), onder de loep te nemen en het verband te leggen tussen *money control* en het bankgeheim, meer bepaald aan de hand van het 'Valentijn-arrest' van het Grondwettelijk Hof (GH, 14 februari 2013, nr. 7/2013). Alvorens af te ronden, zal hij een parallel trachten te trekken tussen *money control* en het vermogenskadaster en nagaan hoe de tekortkomingen van *money control* kunnen worden aangepakt door minimale waarborgen in te bouwen, zoals de naleving van artikel 22 van de Belgische Grondwet, artikel 22 van de AVG en artikel 8 van het Europees Verdrag van de Rechten van de Mens.

Alle bankrekeningen, tegoeden en financiële contracten (inclusief effectenrekeningen) van alle Belgen zullen in de databank worden opgenomen.

Zoals de minister van Financiën heeft aangestipt, zullen de gegevens van het CAP niet alleen kunnen worden gebruikt bij duidelijke belastingfraude, maar ook door de belastingdienst kunnen worden geraadpleegd bij belastingontwijking of een vermoeden van fraude.

Het lid stelt vast dat het project *chat control* niet dood en begraven is, zoals eerder aangekondigd. Hij merkt op dat de werkgroep die zich buigt over de toepassing van de wet en die belast is met de behandeling van aangelegenheden in verband met wetgevingsactiviteiten,

que le champ d'action a été élargi aux crypto-monnaies et aux comptes-titres.

Il reviendra plus loin dans son intervention sur la jurisprudence de la CJUE (les arrêts *Dun & Bradstreet* (C-203/22) et *Schuffa Holding* (C-634/21) du 7 décembre 2023), sur l'impact de l'intelligence artificielle sur la fiscalité, notamment le scandale des allocations familiales aux Pays-Bas ("toeslagenaffaire") et l'*E-kasa* en Slovaquie. Ce système de caisses enregistreuses électroniques connecte obligatoirement les entreprises qui acceptent des paiements en espèces ou par carte aux portails de l'administration fiscale slovaque. Mis en place en juillet 2019, il vise à combattre la fraude fiscale en permettant le suivi en ligne du détail des transactions. Ce système a été annulé par la Cour constitutionnelle slovaque.

Il poursuivra par une analyse de l'IA-Act de l'Union européenne (Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence.

Il sera ensuite temps d'examiner le fonctionnement de *money control* et de ses 3 piliers: l'exploration de données (*data mining*), SAQ software et les fiches DAM (*Digital Asset Management*), de faire la relation entre *money control* et le secret bancaire, notamment via l'arrêt Valentijn de la Cour constitutionnelle (CC 14 février 2013, n° 7/2013); il tentera d'établir le parallèle entre *money control* et le cadastre du patrimoine et de voir comment remédier à *money control* en insérant les garanties minimales comme le respect de l'article 22 de la Constitution belge, de l'article 22 du RGPD et de l'article 8 Convention européenne des droits de l'homme, avant de conclure.

Tous les comptes en banque, tous les soldes et tous les contrats financiers (y compris les comptes-titres) de tous les Belges seront repris dans la base de données.

Comme le ministre des Finances l'a rappelé, les données reprises dans le PCC ne seront pas uniquement utilisables en cas de fraude fiscale caractérisée mais susceptible d'être consulté par l'administration fiscale en cas d'évitement de l'imposition ou de suspicion de fraude.

Concernant *chat control*, le membre constate que le projet n'est pas mort et enterré comme on l'avait annoncé. Il fait observer que le groupe "Application de la loi" chargé de traiter les questions relatives aux activités législatives, ainsi qu'à l'activité policière transfrontière et

grensoverschrijdende politieactiviteiten en de aanverwante operationele aspecten binnen de Europese Unie, op 12 november 2025 heeft besloten om het dossier *chat control* op de agenda te plaatsen. Dit werd openbaar gemaakt dankzij de waakzaamheid van journalisten en ngo's. De Raad vreest immers dat de publieke opinie zich opnieuw tegen dat project zal keren.

In het hier besproken wetsontwerp doet de manier waarop de wetgeving tot stand komt vragen rijzen: er wordt weinig ruchtbaarheid aan gegeven, er worden via amendementen sluiks zaken aan toegevoegd, er worden geen hoorzittingen gehouden enzovoort. Dat alles zorgt ervoor dat de publieke opinie geen vat krijgt op het onderwerp.

Het lid zal nader ingaan op de ontstaansgeschiedenis van *chat control* (namelijk wat het project aanvankelijk inhield en waarom het mislukt is), de gevaren van het 2.0-project en de manier waarop transparantie en geïnformeerde burgers weerstand kunnen bieden tegen massasurveillance. Tot slot zal hij ook de link leggen met *money control* en de ingediende amendementen.

Alles is begonnen met de CSAM-verordening van 2022, waarin wordt verwezen naar het voorstel van verordening van de Europese Unie van mei 2022 ter voorkoming en bestrijding van online seksueel misbruik van kinderen (CSAM), ook *chat control* genaamd. Dat voorstel beoogde aanbieders van diensten ertoe te verplichten inhoud met seksueel misbruik van kinderen te detecteren en te melden. Het project deed heel wat stof opwaaien omdat het de persoonlijke levenssfeer en end-to-end versleutelde communicatie zou kunnen aantasten.

Doelstellingen van het voorstel

- Aanbieders van diensten verplichten om online inhoud met seksueel misbruik van kinderen te detecteren, te melden en te blokkeren.
- "Preventie- en beschermingsmaatregelen nemen.
- Verplichtingen opleggen aan aanbieders van diensten, zoals het detecteren en melden van misbruik.

Controverse en huidige toestand

- Massasurveillance: het project krijgt kritiek omdat het zou kunnen leiden tot wijdverspreide surveillance van privécommunicatie (WhatsApp enzovoort).

aux aspects opérationnels connexes au sein de l'Union européenne a, en date du 12 novembre 2025, décidé de remettre le dossier *chat control* à l'agenda. Ceci a pu être rendu public grâce à la vigilance de journalistes et d'ONG. Le Conseil a en effet peur de voir une nouvelle levée de boucliers contre ce projet dans l'opinion publique.

Dans le projet de loi en discussion, la manière dont la législation est construite interpelle: peu de publicité, introduction en catimini via amendements, pas d'auditions,... ce qui empêche l'opinion publique de s'emparer du sujet.

Le membre rappellera plus avant la genèse de *chat control* (ce qu'était le projet au départ et comment il a échoué), quels sont les dangers du projet 2.0, comment la transparence et l'information citoyenne peuvent résister à une surveillance de masse et, enfin, il fera le lien avec *money control* et les amendements déposés.

Tout a débuté avec le "Règlement CSAM 2022" qui fait référence à la proposition de règlement de l'Union européenne présentée en mai 2022 pour prévenir et combattre les abus sexuels sur enfants en ligne (CSAM), également appelée "*chat control*". Cette proposition visait à obliger les fournisseurs de services à détecter et signaler les contenus d'abus sexuels sur enfants, et ce projet a suscité d'importantes controverses en raison de son potentiel d'atteinte à la vie privée et aux communications chiffrées de bout en bout.

Objectifs de la proposition

- Obliger les fournisseurs de services à détecter, signaler et bloquer les contenus d'abus sexuels sur enfants en ligne.
- Mettre en place des mesures de prévention et de protection nationales.
- Mettre en place des obligations pour les fournisseurs de services, telles que la détection et le signalement des abus.

Controverses et état actuel

- Surveillance de masse: Le projet a été critiqué pour potentiellement entraîner une surveillance généralisée des communications privées (WhatsApp, ...).

— End-to-endversleuteling: het oorspronkelijke voorstel was niet verenigbaar met end-to-end-versleuteling, omdat het vereiste dat alle communicatie vóór de verzending zou worden geanalyseerd.

— Verwerping: een voorstel om alle foto's en video's automatisch te analyseren werd in 2024 door de lidstaten verworpen.

— Huidige status: in 2025 blijft het voorstel voer voor debat, aangezien geen consensus werd bereikt.

De heer Van Quickenborne trekt een parallel met het huidige wetsontwerp: het algemeen toezicht op privécommunicatie werd afgewezen. Quid dan met de bankrekeningen? Chat Control beoogde een toezicht op persoonlijke berichten; *money control* beoogt een datawarehouse (gegevensmagazijn) tot stand te brengen, een gecentraliseerd referentiesysteem dat gegevens uit meerdere bronnen samenbrengt.

De parallel is getrokken: elke beweging wordt geregistreerd, zoals bij het zogenaamde sleepnet, die onderzoeksmethode van de politie waarbij een bepaald gebied wordt afgezet om vervolgens via grootschalige controles en verificaties verdachten op te pakken. Iedereen kan worden verdacht, omdat het spectrum zo breed is. Het risico bestaat dat het vermoeden van onschuld plaatsmaakt voor het vermoeden van schuld. De spreker vindt zulks volkomen onevenredig en tal van fiscale deskundigen delen dat standpunt.

Hoe werd chat control van de agenda gehaald?

Dankzij vooruitgang op drie fronten:

1. De juridische dienst van de Raad heeft in 2023 een advies uitgebracht over de CSAM-verordening uit 2022, teneinde na te gaan of die in overeenstemming is met het Handvest van de grondrechten van de Europese Unie (artikelen 7 en 8). Daarin staat dat er “een ernstig risico [bestaat] van niet-naleving van het evenredigheidsbeginsel, voor zover de opsporingsbevelen de algemene en ongedifferentieerde toegang tot de inhoud van interpersoonlijke communicatie door een specifieke dienstenaanbieder zouden vereisen en zonder onderscheid van toepassing zouden zijn op alle personen die van die specifieke dienst gebruikmaken, zonder dat deze personen zich – zelfs indirect – in een situatie bevinden die tot strafvervolging kan leiden.”

De GBA heeft dezelfde bewoordingen gebruikt als de juridische dienst van de Raad.

De juridische dienst van de Raad verwijst in zijn advies naar het arrest-*La Quadrature du Net*, waarin het Hof

— Chiffrement: La proposition initiale était incompatible avec le chiffrement de bout en bout, car elle exigeait l'analyse de toutes les communications avant leur transmission.

— Rejet: Une proposition nécessitant l'analyse automatique de toutes les photos et vidéos a été rejetée par les États membres en 2024.

— Statut actuel: en 2025, la proposition reste en discussion, car un consensus n'a pas été trouvé.

M. Van Quickenborne fait le parallèle avec le projet de loi actuel: la surveillance généralisée des communications privées a été recalée, qu'en sera-t-il alors des comptes en banque? C'est le canal qui était visé avec *chat control*; ici, avec *money control* c'est le *data warehouse* (l'entrepôt de données), un référentiel centralisé qui rassemble des données provenant de sources multiples.

Le parallèle est fait: chaque mouvement est répertorié, comme la pratique policière du “filet de pêche” (“*sleep-net*”), consistant à boucler une zone afin d'appréhender des suspects grâce à des contrôles et des vérifications à grande échelle. Chacun peut être suspect tant le spectre est large: il y a un risque que la présomption d'innocence fasse place à la présomption de culpabilité. L'intervenant estime que c'est complètement disproportionné. C'est aussi l'avis de nombreux experts en matière de fiscalité.

Comment chat control a été retiré de l'agenda?

Grâce à des avances sur 3 fronts:

1. Le service juridique du Conseil a rendu un avis en 2023 sur le Règlement CSAM 2022 afin de vérifier sa conformité avec la Charte des droits fondamentaux de l'Union européenne (articles 7 et 8). Il a estimé “qu'il existe un risque grave de non-respect du principe de proportionnalité dans la mesure où les injonctions de détection exigeraient un accès généralisé et indifférencié au contenu des communications interpersonnelles par un fournisseur de services déterminé et s'appliqueraient sans distinction à toutes les personnes utilisant ce service spécifique, sans que ces personnes ne se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales”.

L'APD a utilisé les mêmes mots que le service juridique du Conseil.

Le service juridique du Conseil a fait mention dans son avis de l'arrêt *La Quadrature du Net*, dans lequel

heeft verduidelijkt “dat de bijzonder ernstige inmenging die het gevolg is van een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens (...) en de bijzonder ernstige inmenging die de geautomatiseerde analyse van die gegevens met zich brengt, slechts aan het evenredigheidsvereiste kunnen voldoen in situaties waarin een lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, en op voorwaarde dat de duur van die bewaring tot het strikt noodzakelijke wordt beperkt.”

De spreker trekt een voor de hand liggende parallel tussen *chat control* en *money control*.

2. De Europese Toezichthouder voor gegevensbescherming (EDPS) en het Europees Comité voor gegevensbescherming (EDPB) zijn tot dezelfde conclusie gekomen: algemene toegang tot de inhoud van communicatie door overheidsinstanties brengt de kern van het recht op privacy in gevaar. Een uitzondering op het recht op communicatiegeheim mag niet de regel worden. De instanties in kwestie benadrukken het belang van end-to-endversleuteling als basis voor veilige communicatie op internet, een fundamentele bouwsteen voor vertrouwelijkheid en voor de vrijheid van meningsuiting. Massaal ongedifferentieerd toezicht betekent de Rubicon oversteken.

3. Het protest in de publieke opinie, op sociale media en de politieke gevolgen daarvan.

De spreker hoopt oprecht dat een schokgolf door de samenleving zal gaan en dat eenieder tot het besef zal komen dat dergelijke maatregelen niet mogen worden aangenomen, daar ze de fundamentele vrijheden aantasten.

Alle bankrekeningen, alle saldi (twee keer per jaar) en alle financiële contracten van alle Belgen zullen in de databank worden opgenomen. Bij de minste beweging die afwijkt van de gewoonten van een burger bestaat het risico dat de fiscus de betrokkene om uitleg vraagt, wat volstrekt onevenredig is.

In Europa zijn campagnes als *Stop chat control* ontstaan, alsook de website *Fight chat control* en de coalitie *Stop Scanning Me*, met video's, infographics en opinieartikelen van deskundigen op sociale media, in de pers enzovoort. Het debat is in de publieke opinie losgebarsten met een centrale vraag: willen wij dat onze WhatsAppberichten systematisch door algoritmen worden gelezen?

De heer Van Quickenborne herinnert eraan dat velen in het federale Parlement voorstander waren van *chat*

la Cour a précisé que “l’ingérence particulièrement grave que comporte l’analyse automatisée généralisée et indifférenciée des données relatives au trafic et des données de localisation ne peut satisfaire à l’exigence de proportionnalité que dans des situations dans lesquelles un État membre est confronté à une menace grave pour la sécurité nationale qui s’avère réelle et actuelle ou prévisible, et à la condition que la durée de conservation soit limitée au strict nécessaire”.

Le membre fait un parallèle évident entre *chat control* et *money control*.

2. Le Contrôleur européen de la protection des données (CEPD) et le Comité européen de la protection des données (EDPB) sont arrivées à la même conclusion: l'accès général au contenu des communications par les autorités publiques compromet l'essence même du droit à la vie privée. Une exception au secret des communications ne doit pas devenir la règle; ils soulignent l'importance du chiffrement de bout en bout comme la base de la sécurité sur Internet, fondement de la confidentialité et de la liberté d'expression. La surveillance de masse reviendrait à franchir le Rubicon.

3. La contestation dans l'opinion publique, sur les réseaux sociaux et les conséquences politiques qui en ont résulté.

Il espère sincèrement qu'un sursaut se produira au sein de la société et que tout un chacun se rendra compte que ces dispositions liberticides ne peuvent être adoptées.

Tous les comptes en banque, tous les soldes (deux fois par an) et tous les contrats financiers de tous les Belges seront repris dans la banque de données. Dès qu'un mouvement sortant des habitudes d'un citoyen sera détecté, il y a un risque que le fisc sollicite une demande d'explication, ce qui est tout à fait disproportionné.

En Europe, des campagnes *Stop chat control* ont vu le jour, de même qu'un site web *Fight chat control*, la coalition *Stop scanning me*, des vidéos, des infographies et des tribunes d'experts sur les réseaux sociaux, dans les médias... Le débat s'est installé dans l'opinion publique avec une question centrale: voulons-nous que nos messages WhatsApp soient systématiquement lus par des algorithmes?

M. Van Quickenborne rappelle qu'au sein du Parlement fédéral, beaucoup étaient favorables à *chat control* mais

control, maar dat de meningen als gevolg van de debatten zijn geëvolueerd. Zelfs de N-VA is van mening veranderd, alleen cd&v is voorstander van *chat control* gebleven.

Veel Europese landen (Duitsland, Nederland, Denemarken enzovoort) zijn zich ertegen gaan verzetten en brachten verandering in de situatie: er was geen gekwalificeerde meerderheid meer die de tekst steunde.

Het lid stelt vast dat de verschillende adviezen van de instanties en het protest van burgers uiteindelijk de doorslag hebben gegeven. De heer Van Quickenborne beschouwt dit als een daad van verzet; het was David tegen Goliath.

Hij betreurt dat *chat control 2.0* via een achterpoortje weer op de Europese agenda staat. Er is weinig informatie daarover te vinden. De belangrijkste verandering is dat het scannen op vrijwillige basis zal gebeuren. Dienstverleners die worden geacht een hoog risico te hebben, moeten alle passende maatregelen nemen om dat risico te beperken.

Wie bepaalt wat een hoog risico is? Elke chat- of communicatiedienst die veel wordt gebruikt, heeft een hoog risico. Hoe meer gebruikers, hoe hoger het risico.

Wie bepaalt wie de nodige maatregelen moet nemen om de risico's te beperken? Dat is de Europese toezichthouder, de Europese Commissie. Dat kan heel ver gaan: wie niet scant, kan worden bestraft, wat in de praktijk neerkomt op verplichte *chat control*.

Voorts blijft het niet bij het scannen van foto's en video's: ook tekstgesprekken en metagegevens kunnen door algoritmen worden geanalyseerd. Zo kan AI tekstgesprekken scannen op basis van verdachte woordcombinaties. Er bestaat een risico op 'vals-positieve' resultaten.

Aan de soms wazige grens tussen (verboden) belastingontduiking en (niet-verboden) belastingontwijking, zullen burgers last krijgen, soms enkel op basis van woorden die het algoritme gebruikt. Wie wordt geconfronteerd met vermoedens van fraude moet zich verantwoorden. In geval van vals-positieve resultaten kan dat op verschillende niveaus ernstige gevolgen hebben. Zulks is niet proportioneel.

Door *chat control* bestaat het risico dat vals-positieve resultaten worden genormaliseerd en dat duizenden mensen worden beschuldigd van misbruik van minderjarigen, terwijl ze niets verkeerd hebben gedaan. Dat is precies wat er in Nederland gebeurde met de toeslagenaffaire: duizenden mensen werden op basis van een algoritme beschuldigd van het onrechtmatig ontvangen

qu'à la lumière des débats, les opinions ont évolué. Même la N-VA a changé d'avis, seul le cd&v a maintenu sa position initiale favorable à *chat control*.

De nombreux pays européens (Allemagne, Pays-Bas, Danemark, ...) ont commencé à s'opposer et à faire bouger les lignes: il n'y avait plus de majorité qualifiée pour soutenir le texte.

Il observe que les différents avis de ces instances et la contestation citoyenne ont au final comptés. Pour M. Van Quickenborne, il s'agit d'un acte de résistance. Comme David contre Goliath.

Il déplore que, par une porte dérobée, *chat control 2.0* revienne à l'agenda européen. Peu d'information circule à ce sujet. Le changement principal est que le scanning se fera sur une base volontaire. Les prestataires de services considérés comme présentant un risque élevé doivent prendre toutes les mesures appropriées pour limiter ce risque.

Qui détermine ce qu'est un risque élevé? Chaque *chat* ou service de communication qui est fort utilisé est à haut risque. Plus il y a d'utilisateurs, plus le risque est élevé.

Qui détermine qui doit prendre les mesures appropriées pour limiter les risques? C'est le contrôleur européen, la Commission européenne. Cela peut aller très loin: celui qui ne scanne pas peut être sanctionné, cela revient dans les faits à un *chat control* obligatoire.

Une deuxième caractéristique est que cela ne limite plus au scanning de photos et de vidéos mais aussi au chat de texte et aux métadonnées qui peuvent être analysées par des algorithmes. L'IA peut ainsi scanner des textes de conversation sur la base de combinaison de mots suspects. Il y a un risque de "faux positifs".

On se retrouve dans une frontière tenue entre fraude fiscale et évitement fiscal, ce qui n'est pas interdit, parfois juste à cause de mots utilisés par les algorithmes. Si certaines personnes sont confrontées à des présomptions de fraude, c'est à eux de se justifier. Dans les cas de "faux positifs", cela peut avoir de lourdes conséquences à plusieurs niveaux. Ce n'est pas proportionnel.

Chat control menace de normaliser ces "faux positifs" en accusant des milliers de personnes d'abuser de mineurs alors qu'ils n'ont rien à se reprocher. C'est exactement ce qui s'est passé aux Pays-Bas avec les "toeslagenaffaire": plusieurs milliers de personnes ont été accusées de percevoir des allocations sociales indues à cause d'un algorithme, en étant erronément

van sociale uitkeringen en werden onterecht bestraft, waardoor ze sociaal en economisch in een kwetsbare situatie terechtkwamen. De regering moest aftreden en de belastingdienst werd veroordeeld.

Chat control vertoont nog een ander probleem, namelijk de leeftijds- en anonimiteitscriteria. Men dient te kunnen bepalen wie meerderjarig is en wie niet en zich te kunnen identificeren (via gezichtsherkenning of andere technologie).

In het pseudonimiseringsproces van *money control* worden de gegevens waarmee een individu rechtstreeks kan worden geïdentificeerd (zoals zijn naam) door een onrechtstreekse identifier vervangen (zoals een pseudoniem of een unieke code). Daardoor kunnen persoonsgegevens worden verwerkt met een minimumrisico voor de bewuste personen zelf, aangezien ze zonder de bijbehorende, afzonderlijk bewaarde informatie niet kunnen worden geïdentificeerd. Gepseudonimiseerde gegevens blijven persoonsgegevens waarop de AVG van toepassing is, maar door de algoritmes worden bepaalde profielen waarop verdachte bewegingen zijn geregistreerd, opgespoord, waarna de sleutel om de betrokkene te identificeren, ter beschikking wordt gesteld. De gelijkenis met hoe *chat control 2.0* werkt, is treffend. Het risico bestaat dat ondernemerschap, maar ook klokkenluidersinitiatieven en journalistiek onderzoek daardoor worden afgeremd. En wie in een gewelddadige gezinsrelatie zit of activisten van allerlei aard zullen al helemaal geen actie meer durven te ondernemen.

De volgende stap zal *Doctor Control* zijn, die het gemunt zal hebben op wie een medisch of psychologisch dossier heeft. Men zal zich baseren op de bewaarde voorschriften van alle patiënten en artsen, met de eraan verbonden risico's.

De anonimisering creëert in de feiten geen daadwerkelijke anonimiteit. Nochtans zijn anonieme communicatie en anonieme bankrekeningen geen luxeproducten voor trollen, maar fungeren ze als veiligheidsinstrumenten en fundamentele bouwstenen voor het vertrouwen in de democratie.

Volgens de spreker zitten er veel tegenstrijdigheden in de teksten en bij ontstentenis van de nodige verduidelijking via de toelichting bij de artikelen is een aanpassing van het wetsontwerp op zijn plaats.

Bart Preneel, een van de deskundigen ter zake, cryptoloog en hoogleraar aan de Katholieke Universiteit Leuven, waar hij directeur is van de COSIC-groep (*Computer Security and Industrial Cryptography*), heeft zich zeer snel tegen *chat control* verzet. Zijn mening over dit wetsontwerp zou nuttig zijn.

sanctionnées, les fragilisant d'un point de vue social et économique. Le gouvernement a du démissionner et l'administration fiscale a été condamnée.

Autre problème rencontré avec *chat control*: les critères d'âge et d'anonymat. Il faut pouvoir déterminer qui est majeur ou non et s'identifier (Face Id ou autre).

Pour *money control*, la pseudonymisation est un processus qui consiste à remplacer les données directement identifiantes d'un individu (comme son nom) par un identifiant indirect (comme un pseudonyme ou un code unique). Elle permet de traiter des données personnelles tout en réduisant les risques pour les personnes, car elles ne peuvent plus être identifiées sans des informations complémentaires qui sont conservées séparément. Les données pseudonymisées restent des données personnelles soumises au RGPD mais, à cause des algorithmes, certains profils avec des suspicion de mouvements seront mis à jour et la clé sera donnée pour pouvoir identifier le sujet. Le parallèle est évident avec *chat control 2.0*. Cela risque de freiner à la fois l'esprit d'entreprise, d'une part, et les lanceurs d'alerte & les journalistes, d'autre part. Sans parler des personnes qui sont dans une relation familiale violente ou des activistes de tout ordre.

Viendra ensuite *Doctor Control* qui visera les personnes avec un profil médical ou psychologique en conservant les prescriptions de tous les patients et médecins avec le risques que cela induit.

L'anonymisation n'en est pas une en réalité: communications anonymes et comptes en banque anonymes ne sont pas un produit de luxe pour trolls mais un garde-fou et les fondements de la confiance en la démocratie.

L'intervenant estime que les textes sont contradictoires sur bien des aspects et, quand la justification des articles n'apporte pas les éléments de clarification nécessaires, il y a lieu d'adapter le projet de loi.

Bart Preneel, un des experts en la matière, cryptologue et professeur à la Katholieke Universiteit Leuven où il est directeur du groupe COSIC (*Computer Security and Industrial Cryptography*), s'est très rapidement opposé à *chat control*. Il serait utile de l'entendre sur ce projet de loi.

De heer Van Quickenborne verzoekt de minister om de zeven problematische leden van het artikel in kwestie in te trekken, opdat vooruitgang kan worden geboekt en kan worden gestemd over de overige diverse bepalingen van dit wetsontwerp. Hij vreest dat *money control* de ontbrekende schakel in de totstandkoming van een vermogenskadaster zal zijn, wat het enthousiasme van de linkse partijen over dit wetsontwerp verklaart. De houding van de heer Van Quickenborne is er een van krachtadig principiële verzet tegen zowel de inhoud als de gebruikte methode (stiekem door de meerderheid ingediende slecht geformuleerde amendementen met vrome wensen in plaats van een degelijke normatieve tekst). Naast de eerste en de laatste versie zijn er zelfs nog verscheidene tussenversies geweest.

De spreker verheugt zich erover dat de heer Coenegrachts overall in Limburg, van Bilzen tot in Peer en Pelt *money control* gaat uitleggen, zoals Yves Leterme in de tijd ook heeft gedaan, van Aarlen tot in De Panne, om de regering Verhofstadt te bestrijden. De heer Coenegrachts zal *money control* uitleggen totdat burgerprotest er is.

In het kader van *chat control 1.0* is het niet de rechter die de verordening heeft vernietigd, noch de Europese Commissie op eigen initiatief, maar de publieke druk met landen zoals Duitsland, Oostenrijk en Nederland die alarm hebben geslagen.

Om dat mechanisme van burgerprotest te doen werken moet de procedure het toelaten. In dit opzicht uit de heer Van Quickenborne zijn waardering tegenover de voorzitter van de commissie Financiën die het mogelijk maakt om een parlementair debat te voeren. Hij verwacht ook de antwoorden van de meerderheid op de vragen die werden gesteld. Wel geen antwoorden in de zin dat de spreker zijn rijke vrienden wil beschermen en dat het alleen maar om georganiseerde fraude gaat.

De spreker merkt op dat het feit dat een nieuw debat over *chat control 2.0* zal worden georganiseerd de lidstaten in de Raad opnieuw zal doen twifelen. Er zouden opnieuw privacy-adviezen worden geleverd waarvan de inhoud gemakkelijk te raden is.

Wetsontwerp *money control*

Money control komt volgens de heer Van Quickenborne neer op de invoering van een *chat control* in België. Hij haalt dit dossier in deze commissie uitdrukkelijk aan omdat België iets wil invoeren dat *mutatis mutandis* uit dezelfde logica is gesneden. Het doel van het systeem is om de overheid in staat te stellen om massaal gegevens te analyseren.

M. Van Quickenborne invite le ministre à retirer les sept alinéas qui posent problème pour avancer et voter le reste des dispositions diverses de ce projet de loi. Il craint que *money control* sera le chaînon manquant pour créer un cadastre du patrimoine, ce qui explique l'enthousiasme des partis de gauche pour ce projet. Il s'agit ici d'une opposition de principe exprimée avec force, tant sur le fond que sur la méthode utilisée, avec des amendements introduits par la majorité en catimini et mal formulés (des vœux pieux et non un texte normatif). Il y a même eu des versions différentes entre la première et la dernière mouture.

L'intervenant se réjouit que M. Coenegrachts s'engage à expliquer le "*money control*" partout dans le Limbourg, de Bilzen à Peer et Pelt, comme Yves Leterme autrefois, d'Aarlen à La Panne, pour lutter contre le gouvernement Verhofstadt. M. Coenegrachts expliquera le "*money control*" jusqu'à ce que les citoyens protestent.

En ce qui concerne le *chat control 1.0*, le règlement n'a pas été annulé par un juge, ni par la Commission européenne de sa propre initiative, mais bien sous la pression publique exercée par des pays tels que l'Allemagne, l'Autriche et les Pays-Bas, qui ont tiré la sonnette d'alarme.

Pour que ce mécanisme de protestation citoyenne fonctionne, la procédure doit le permettre. À cet égard, M. Van Quickenborne exprime sa gratitude au président de la commission des Finances, qui permet qu'un débat parlementaire ait lieu. Il attend également les réponses de la majorité aux questions posées. Il espère toutefois qu'il ne s'agira pas de réponses soutenant que l'intervenant souhaite protéger ses riches amis et qu'il ne s'agit que d'une fraude organisée.

L'intervenant fait observer que le fait qu'un nouveau débat sur *chat control 2.0* sera organisé sèmera à nouveau le doute parmi les États membres au sein du Conseil. De nouveaux avis sur la protection de la vie privée, dont le contenu est facile à deviner, devraient être rendus.

Projet de loi instaurant le *money control*

M. Van Quickenborne estime que le *money control* revient à introduire un *chat control* en Belgique. Il évoque expressément ce dossier au sein de cette commission, car la Belgique souhaite introduire un système qui, *mutatis mutandis*, s'appuiera sur la même logique. L'objectif de ce système est de permettre aux pouvoirs publics d'analyser massivement des données.

In dit verband verwijst hij naar de andere rol die de heer Wim Van der Donckt (N-VA) tijdens de vorige legislatuur heeft gespeeld toen hij in de oppositie zat. Toen heeft hij in het Parlement duidelijk durven stellen dat de controle van de banken op de PEP's (*Politically Exposed Persons*) te verregaand was. Zozeer zelfs dat op een bepaald ogenblik een van de rekeningen van de heer Van der Donckt geblokkeerd werd omdat de fiscus vragen had gesteld. Achteraf bleek dat er niks aan de hand was, maar met de invoering van *money control* is het PEP in het kwadraat op de hele bevolking. De spreker waarschuwt dus voor het feit dat we zoiets niet aan het land kunnen doen.

Wat *chat control* is voor de gesprekken is *money control* voor onze bankrekeningen en financiële transacties met een duidelijke rode draad: men gaat van gerichte controles op basis van concrete aanwijzingen naar algoritmische massasurveillance.

Wat in deze verontrustend is, is dat het ingekapseld is in een wet houdende diverse bepalingen waardoor het voor de publieke opinie niet interessant is en het ook niet apart wordt behandeld. De zaken zouden helemaal anders zijn als dit wetsontwerp de titel had gekregen van "wet tot invoering van *money control*" of, zoals aangestipt door minister Jan Jambon, "wetsontwerp tot invoering van een *Deus Tax Machina*".

In dit verband verwijst de heer Van Quickenborne naar de toekomstige verdediging van een doctoraatsthesis door David Hadwick aan de Universiteit van Antwerpen met als titel: "*Deus Tax Machina: The use of AI by tax administrations and its implications for taxpayers' fundamental rights in the EU*". Het gaat dus over artificiële intelligentie en de rechten van belastingplichtigen. Dit is ook het punt dat hier behandeld wordt.

Voorts benadrukt de spreker dat er in dit wetsontwerp geen rekening gehouden werd met de adviezen van de Raad van State en van de Gegevensbeschermingsautoriteit. Te noteren valt ook dat er geen grote publieke consultatie is geweest, geen brede mediacampagne en geen maatschappelijke dialoog.

Als men deze tekst per se wil doorvoeren, is er nood aan een volwaardig debat met adviezen en hoorzittingen, zoals de spreker zelf heeft gedaan met zijn dataretentiewet. Het debat in het kader van deze dataretentiewet ging over het feit dat als iemand belt, de metadata bijgehouden worden door de operatoren en met de politie kunnen worden gedeeld.

Die wet was echter proportioneel en er heeft toen een debat plaatsgevonden met parlementaire vragen die tot iets hebben geleid. Mevrouw Sophie De Wit

À cet égard, l'intervenant évoque l'autre rôle joué par M. Wim Van der Donckt (N-VA) lorsqu'il était dans l'opposition, sous la législature précédente. À l'époque, il avait osé affirmer clairement au Parlement que le contrôle des PEP (*Politically Exposed Persons*) exercé par les banques allait trop loin, à tel point qu'à un moment donné, l'un des comptes de M. Van der Donckt a été bloqué parce que le fisc avait posé des questions à son sujet. Il est ensuite apparu que tout était normal, mais le *money control* ira beaucoup plus loin que le PEP pour l'ensemble de la population. L'intervenant souligne qu'il n'est pas acceptable de faire cela à notre pays.

Money control sera pour nos comptes bancaires et nos transactions financières ce que le *chat control* est pour les conversations, avec un fil conducteur clair, à savoir une évolution des contrôles ciblés sur la base d'indices concrets vers une surveillance algorithmique de masse.

Ce qui est inquiétant dans cette situation, c'est que le *money control* soit encapsulé dans une loi portant des dispositions diverses, ce qui le rend inintéressant pour l'opinion publique et implique qu'il ne fait pas l'objet d'un examen distinct. Il en irait tout autrement si le projet de loi à l'examen avait été intitulé "loi instaurant le *money control*" ou, comme l'a dit le ministre Jan Jambon, "projet de loi instaurant un *Deus Tax Machina*".

À ce propos, M. Van Quickenborne renvoie à la future défense d'une thèse de doctorat intitulée "*Deus Tax Machina: The use of AI by tax administrations and its implications for taxpayers' fundamental rights in the EU*" par David Hadwick à l'Université d'Anvers. Cette thèse porte donc sur l'intelligence artificielle et sur les droits des contribuables, comme le débat en cours au sein de cette commission.

L'intervenant souligne en outre que le projet de loi à l'examen ne tient pas compte des avis du Conseil d'État et de l'Autorité de protection des données. Il convient également de noter l'absence de consultation publique à grande échelle, d'une large campagne médiatique, et de tout dialogue sociétal.

Si l'on tient absolument à adopter ce texte, il faudra mener un réel débat à la lumière d'avis et d'auditions, comme l'a fait l'intervenant lui-même pour sa loi sur la conservation des données. Dans ce cadre, le débat portait sur le fait que lorsqu'un utilisateur passe un appel, ses métadonnées sont conservées par les opérateurs et peuvent être partagées avec la police.

Cette loi était toutefois proportionnée et elle a fait l'objet d'un débat au cours duquel ont été posées des questions parlementaires qui ont porté leurs fruits. Mme Sophie

(N-VA) – toen in de oppositie – had gezegd dat de wet geen stand zou houden, maar dat is niet het geval geweest, in tegenstelling tot dit wetsontwerp dat er niet zal komen omdat het een screening van alle bankrekeningen inhoudt. De aanpak met dit wetsontwerp kan vergeleken worden met de problematiek van huiselijk geweld: niemand zou het proportioneel vinden dat in elk huis een camera wordt geplaatst om dat tegen te gaan. In deze is het nochtans wat de regering wil doen met onze betalingen en financiële contracten.

De heer Van Quickenborne uit vervolgens kritiek op de manier waarop de regering deze wet wil doordrukken, namelijk stiekem via amendementen en zonder debat. Zoals aangestipt door de spreker neemt niemand het woord. De andere parlementsleden doen de moeite niet om te spreken. Ofwel omdat ze niet durven spreken of omdat ze moeten zwijgen. En als men moet zwijgen in de politiek, omwille van de participatie, dan is dit parlement monddood gemaakt. Het is dus wachten op het eerste parlements lid dat zal durven zeggen dat het genoeg is geweest. Dit heeft Mathieu Michel (MR) als voormalig Staatssecretaris voor privacy in mei wel tegen de minister durven zeggen, maar hij is monddood gemaakt door de eerste minister van dit land.

Dat een partij als de N-VA, die zegt op te komen voor de hardwerkende Vlaming, de rekeningen van al die mensen wil screenen, omdat ze verdacht worden van fraude, is voor de spreker onbegrijpelijk.

Wat men hier aan het doen is, is om in de laatste dagen van deze regering – want de kans dat die regering valt is groter dan mensen zouden denken – nog snel een aantal wetten erdoor te duwen. Een daarvan is *money control*.

Volgens minister Jambon staan 150 vragen te wachten op een antwoord en zijn er nog een aantal wetsontwerpen in de pipeline.

De oplossing is duidelijk: dit punt moet gewoon uit de tekst gehaald worden.

Als de minister dat niet doet, zal hij verantwoordelijk zijn voor het feit dat alles geblokkeerd geraakt. Het is immers zijn keuze geweest om dit niet als een apart wetsontwerp te behandelen.

De spreker wijst er ook op dat deze manier van werken vergelijkbaar is met de methode van Arizona, waarbij men alles aan alles koppelt, en er op den duur niets mee gebeurt. Hij haalt het voorbeeld aan van het Zomerakkoord. Er was een akkoord met historische elementen: versoepeling van nachtarbeid, meer overuren, flexi-jobs

De Wit (N-VA) – qui était alors dans l'opposition – avait indiqué que cette loi ne ferait pas long feu, mais elle a résisté, contrairement au projet de loi à l'examen, qui ne verra pas le jour, car il prévoit le contrôle de tous les comptes bancaires. L'approche du projet de loi à l'examen peut être comparée à la problématique de la violence domestique. En effet, personne ne pense qu'il serait proportionné d'installer une caméra dans chaque foyer pour lutter contre ce problème. C'est pourtant ce que le gouvernement souhaite faire en ce qui concerne nos paiements et nos contrats financiers.

M. Van Quickenborne dénonce ensuite la procédure adoptée par le gouvernement pour faire passer cette loi de force, c'est-à-dire une procédure menée en catimini, par le biais d'amendements et sans débat. Comme l'a souligné l'intervenant, personne ne prend la parole. Les autres députés ne prennent pas la peine de s'exprimer, soit parce qu'ils n'osent pas parler, soit parce qu'ils doivent se taire. Et si c'est le cas, en raison de la participation, alors ce parlement est réduit au silence. Il faudra donc attendre le premier député qui osera dire que la coupe est pleine. Mathieu Michel (MR), ancien secrétaire d'État chargé de la protection de la vie privée, a osé le dire au ministre en mai, mais il a été réduit au silence par le premier ministre de notre pays.

L'intervenant ne peut pas comprendre qu'un parti tel que la N-VA, qui prétend défendre les Flamands qui travaillent dur, veuille contrôler leurs comptes au motif qu'ils sont suspectés de fraude.

Ce que l'on est en train de faire ici, alors que ce gouvernement vit ses derniers jours – car la probabilité que ce dernier tombe est plus grande que certains le pensent – c'est de faire passer en toute hâte une série de lois au rang desquelles figure *money control*.

Selon le ministre Jambon, 150 questions sont en attente de réponse et plusieurs projets de loi sont toujours à l'étude.

La solution est claire: ce point doit tout simplement être retiré du texte.

Si le ministre ne le fait pas, il sera responsable du blocage de l'ensemble du dossier. Car c'est lui qui a choisi de ne pas traiter cette question dans un projet de loi distinct.

L'intervenant souligne également que cette façon de travailler est comparable à la méthode de l'Arizona, qui consiste à tout lier à tout et où rien ne se passe au final. Il cite l'exemple de l'accord de l'été. Il s'agissait d'un accord comportant des éléments historiques: assouplissement du travail de nuit, augmentation des heures

voor alle gepensioneerden in alle sectoren. Open Vld was bereid om dit te steunen, maar uiteindelijk kwam er niks in het Parlement omdat alles aan alles gekoppeld is. Dat is hetzelfde hier. Dat is de methode De Wever en die methode leidt tot niks. Grote verklaringen, grote beloftes, maar nul realisaties. En intussen zal België het slechtste begrotingstekort van Europa krijgen en zal de fout bij Open Vld worden gelegd. Straks is het hetzelfde verhaal voor *money control* volgens de spreker: dat zal in de schoenen van Open Vld geschoven worden omdat te weinig gedaan werd om fraude te bestrijden.

Welke lessen kunnen we uit *chat control* trekken?

Wat hebben we geleerd met *chat control*?

— Ten eerste, algemene screening is een rode lijn.

De juridische dienst van de Raad heeft benadrukt dat algemene en ongedifferentieerde screening van communicatie zonder individuele verdenking, onverenigbaar is met de Europese grondrechten. Dit komt gevaarlijk dichtbij bij het aantasten van het recht op privacy.

De logica van die algemene ongedifferentieerde screening is exact dezelfde bij *money control*. Niet op de berichten, maar op de financiële gegevens. Het idee van alle berichten algemeen en ongedifferentieerd te onderzoeken om kindermisbruik op te sporen, is exact hetzelfde als alle bankrekeningen, alle saldi te onderzoeken op zoek naar misbruik.

Het betekent dus dat dit soort ongedifferentieerde controle tot misbruik zal leiden. En een systeem waarbij de overheid of algoritmes standaard alle rekeningen en transacties doorlicht om verdachte patronen te zoeken, is conceptueel identiek aan *chat control*.

Ann De Boeck, journalist bij *De Morgen* maakt in haar artikel van 18 november 2025 over *money control* de vergelijking tussen *chat control* (waarbij algoritmes worden gebruikt) en *money control* (waarbij er sprake is van verwerking). Zoals aangestipt door de spreker is het verschil eerder semantisch want minister Jambon sprak in zijn amendementen over profilering, wat neerkomt op het zoeken van patronen op basis van algoritmes. Er is dus in de feiten geen verschil.

— Ten tweede, negatieve adviezen zijn geen formaliteit.

supplémentaires, flexi-jobs pour tous les retraités dans tous les secteurs. L'Open Vld était prêt à soutenir cet accord, mais au bout du compte, rien n'a été présenté au Parlement, car tout est lié à tout. C'est pareil cette fois-ci. C'est la méthode De Wever, et cette méthode ne mène à rien: de grandes déclarations, de grandes promesses, mais zéro réalisation. En attendant, la Belgique va se retrouver avec le pire déficit budgétaire d'Europe et la faute en sera attribuée à l'Open Vld. L'intervenant estime qu'il en ira de même pour *money control*: on incriminera l'Open Vld parce que trop peu des mesures ont été prises pour lutter contre la fraude.

Quelles leçons pouvons-nous tirer de *chat control*?

Quels enseignements a-t-on tiré de *chat control*?

— Tout d'abord, le contrôle généralisé est une ligne rouge;

Le service juridique du Conseil a souligné que le contrôle généralisé et indifférencié des communications, sans soupçon individuel, est incompatible avec les droits fondamentaux européens. Cette évolution s'apparente dangereusement à une atteinte au droit au respect de la vie privée.

La logique de ce contrôle généralisé et indifférencié est exactement la même que celle qui s'applique à *money control*. Non pas sur les messages, mais sur les données financières. L'idée d'examiner tous les messages de manière généralisée et indifférenciée afin de détecter les abus commis sur des mineurs est exactement la même que celle qui consiste à examiner tous les comptes bancaires et tous les soldes pour détecter des abus.

Ce type de contrôle indifférencié conduira donc forcément à des abus. Et un système dans lequel les autorités ou les algorithmes scrutent d'office tous les comptes et toutes les transactions à la recherche de profils suspects est conceptuellement identique à *chat control*.

Dans son article du 18 novembre 2025 consacré à *money control*, Ann De Boeck, journaliste à *De Morgen*, établit un parallèle entre *chat control* (qui utilise des algorithmes) et *money control* (qui sous-entend un traitement). Comme l'a souligné l'intervenant, la différence est plutôt sémantique, car le ministre Jambon a évoqué le profilage dans ses amendements, ce qui revient à rechercher des profils sur la base d'algorithmes. Il n'y a donc aucune différence dans les faits.

— Ensuite, les avis négatifs ne sont pas une formalité.

In *chat control* hebben de lidstaten wel geluisterd naar de privacy-toezichthouders en naar de juridische dienst om te vermijden dat het juridisch, politiek en maatschappelijk fout zou lopen. Daarom kwam de voorgestelde verordening *chat control 1.0* er niet door.

Als de Gegevensbeschermingsautoriteit, de Raad van State en andere onafhankelijke organen ernstige bedenkingen hebben bij die grootschalige datamining, dan is het de verantwoordelijkheid en de plicht van de minister om daar gevolgen aan te verbinden. De spreker komt later nog in detail terug op de adviezen van de Raad van State en van de GBA, die hij grondig heeft bestudeerd.

Vervolgens vestigt de heer Van Quickenborne de aandacht op drie elementen die essentieel zijn om een goed debat te voeren.

1. **Wederwoord.** Dit is in deze discussie onbestaand. Minister Jambon had al in de eerste lezing geantwoord. Zijn antwoorden staan opgenomen in het verslag van de commissie Financiën en zullen geciteerd worden door de spreker, maar het zijn eigenlijk halve waarheden en onjuistheden.

2. **Transparantie.** Er is geen transparantie. Om dit te illustreren verwijst de spreker naar de zogenaamde DAM-fiches (*Data Asset Management*) die de essentie van een algoritme vormen. Daarin wordt gezegd hoe men zoekt en wat men zoekt, maar niemand weet precies wat die fiches zijn. Zelfs voor de mensen van de Bijzondere Belastinginspectie (BBI) zijn die onbegrijpelijk. De minister weigert om inzage te geven in die fiches omdat het geen deel uitmaakt van het fiscale dossier en omdat het geheim is. En als die informatie kenbaar wordt gemaakt, zou dat ons economisch systeem kunnen ondergraven en zouden de mensen zich kunnen zo organiseren dat ze geen fout meer plegen. In deze sluit de spreker zich aan bij de heer Lode Vereeck (VB) die het over een "*counterfactual approach*" heeft als onderdeel van Explainable AI. Explainable AI houdt in dat AI toegepast kan worden op een complexe algoritme om het uitlegbaar en transparant te maken. Dit werd ook heel goed uitgelegd door Sylvie de Raedt, docent in belastingrecht aan de Universiteit van Antwerpen. Om het totaal gebrek aan transparantie te illustreren geeft de heer Van Quickenborne het bijvoorbeeld van iemand die vijf bankrekeningen heeft met een bescheiden loon als parlementslid en van wie een dossier naar boven komt. Er is dus een "knipperlicht". Als de betrokkene wil weten hoe zijn dossier naar boven is gekomen, krijgt hij als antwoord dat het in de DAM-fiche zit. Maar de DAM-fiches zijn onbegrijpelijk.

Dans le cadre de *chat control*, les États membres ont écouté les autorités chargées de protéger la vie privée et le service juridique afin d'éviter tout dérapage juridique, politique et social. C'est la raison pour laquelle la proposition de règlement *chat control 1.0* n'a pas été adoptée.

Lorsque l'Autorité de protection des données, le Conseil d'État et d'autres organismes indépendants émettent de sérieuses réserves quant à une exploration des données à grande échelle, il est de la responsabilité et du devoir du ministre d'en tirer les conséquences. L'intervenant reviendra plus tard en détail sur les avis du Conseil d'État et de l'APD, qu'il a étudiés de manière approfondie.

Ensuite, M. Van Quickenborne attire l'attention sur trois éléments essentiels pour mener un débat de qualité.

1. **Répliques:** celles-ci sont inexistantes dans le débat actuel. Le ministre Jambon avait déjà apporté des réponses lors de la première lecture. Ses réponses figurent dans le rapport de la commission des Finances et seront citées par l'intervenant, bien qu'il s'agisse, en réalité, de demi-vérités ou d'informations inexactes.

2. **Transparence:** il n'y en a aucune. Pour le démontrer, l'intervenant renvoie aux "fiches DAM" (*Data Asset Management*) qui constituent le cœur même d'un algorithme. Ces fiches indiquent comment on effectue les recherches et ce qu'on cherche, mais personne ne connaît leur nature exacte. Même les collaborateurs de l'Inspection spéciale des impôts (ISI) les jugent incompréhensibles. Le ministre refuse que nous puissions les consulter parce qu'elles ne font pas partie du dossier fiscal et qu'elles sont couvertes par le secret. Et si ces informations étaient divulguées, elles pourraient saper notre système économique et permettre aux contribuables de s'organiser de façon à ne plus commettre d'infraction. À cet égard, l'intervenant rejoint M. Lode Vereeck (VB), qui évoque une "*counterfactual approach*" comme élément de l'intelligence artificielle explicable. Cette dernière implique que l'intelligence artificielle peut être appliquée à un algorithme complexe pour le rendre explicable et compréhensible. Ce procédé est également très bien expliqué par Mme Sylvie de Raedt, professeure en droit fiscal à l'Université d'Anvers (UA). Pour illustrer l'absence totale de transparence, M. Van Quickenborne cite l'exemple d'un contribuable qui possède cinq comptes bancaires, qui perçoit un modeste salaire de député et dont le dossier fait surface. Il y a donc un "clignotant ou signal d'alerte". Si l'intéressé veut savoir pourquoi son dossier est arrivé sur la table, on lui rétorque que c'est indiqué dans la fiche DAM. Mais ces fiches sont incompréhensibles.

Nog steeds in verband met transparantie komt de spreker terug op de thesis van David Hadwick waarin de betrokkene naar meer dan 100 AI-systemen verwijst en de eis naar voren schuift om wetgeving te maken die daarmee rekening zal houden. Bij het lezen van de 7 alinea's van de minister kan men zich afvragen in hoeverre er rekening gehouden wordt met de vraag tot waarborgen, het tegengaan van *statistical bias* en de verschillende AI-systemen.

De heer Van Quickenborne verwijst ook naar het begrip van *Web Scraping*. Waarover gaat het? Als belastingplichtige bent u verplicht door de wetgeving om bepaalde gegevens met de overheid te delen. Maar daarnaast zijn er ook dingen die u deelt met uw vrienden op de sociale media bijvoorbeeld. *Web Scraping* bestaat erin dat de fiscus uw gedrag zal controleren op basis van uw post op de sociale media. De vraag is of de wet 3 augustus 2012 (wet houdende bepalingen betreffende de verwerking van persoonsgegevens door de Federale Overheidsdienst Financiën in het kader van zijn opdrachten) ervoor zorgt dat *Web Scraping* een legale praktijk is? Volgens expert David Hadwick is de wet van 2012 niet aangepast aan dit soort praktijken zelfs als die nog geen *money control* had ingevoerd. De spreker raadt dus aan om eerst de huidige praktijk te controleren in plaats van nieuwe wetsontwerpen en amendementen te bespreken.

3. Tijd. Om een goed debat te voeren is er tijd nodig. Zolang de heer Van Quickenborne vragen blijft stellen over het dossier en zolang er belangstelling is van de andere collega's betekent dit dat het zinvol is en dat het een ernstig debat is.

De drie sleutelementen voor een goed debat zijn dus: wederwoord, tijd en transparantie.

De heer Van Quickenborne vervolgt zijn uiteenzetting met burgerprotest en wijst er nogmaals op dat burgerprotest alleen werkt als de procedure dat toelaat. Bij *chat control* kwamen de teksten op een bepaald moment wel in de openbaarheid. Adviezen werden gepubliceerd en het debat werd gevoerd.

Hier is het net het omgekeerd. Een technisch ogende bepaling wordt in een groot wetspakket opgenomen, de communicatie is beperkt en er is weinig publieke duiding terwijl het een dossier is met een grote impact en schending van de privacy van alle burgers.

Toujours en matière de transparence, l'intervenant revient sur la thèse de David Hadwick, qui évoque plus de 100 systèmes d'intelligence artificielle et souligne la nécessité d'élaborer une législation qui en tiendra compte. À la lecture des sept alinéas du ministre, on peut se demander dans quelle mesure la question des garanties, la nécessité d'éviter les biais statistiques et la diversité des systèmes d'intelligence artificielle sont prises en compte.

M. Van Quickenborne renvoie également à la notion de *Web Scraping*. De quoi s'agit-il? En tant que contribuable, la législation vous impose de partager certaines données avec l'administration. Parallèlement, il vous arrive de partager certaines informations avec vos amis sur les réseaux sociaux, par exemple. Grâce au *Web Scraping*, ou "moissonnage", le fisc va contrôler votre comportement en fonction des *posts* que vous publiez sur les réseaux sociaux. La question est de savoir si la loi du 3 août 2012 (loi portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions) reconnaît le *Web Scraping* comme une pratique légale. Selon l'expert David Hadwick, la loi de 2012 n'est pas adaptée à ce type de pratique, même avant l'arrivée du *money control*. L'intervenant conseille donc de contrôler d'abord la pratique actuelle au lieu d'examiner de nouveaux projets de loi et des amendements.

3. Le temps. Pour pouvoir mener un débat de qualité, il faut disposer du temps nécessaire. Tant que M. Quickenborne continuera à poser des questions sur ce dossier et que ses autres collègues témoigneront de leur intérêt, cela montera que le débat est pertinent et sérieux.

Les trois éléments clés d'un débat de qualité sont donc les répliques, le temps et la transparence.

M. Van Quickenborne poursuit son intervention en évoquant la contestation citoyenne, et il souligne une nouvelle fois que cette contestation ne fonctionne que si la procédure le permet. Dans le cas de *chat control*, les textes y afférents ont, à un moment donné, été révélés au grand public. En outre, des avis ont été publiés et le débat a été mené.

C'est précisément tout l'inverse de ce qui est fait dans le dossier à l'examen. En effet, une disposition aux allures techniques est inscrite dans un train de mesures volumineux, la communication à ce sujet est restreinte et on ne fait guère preuve de pédagogie à l'égard de la population, alors qu'il s'agit d'un dossier aux répercussions majeures qui portera atteinte au respect de la vie privée de tous les citoyens.

De burgers zullen pas stilstaan bij *money control* nadat het systeem is ingevoerd en gestemd en het zal nooit worden afgeschaft. Als de algoritmische machine in gang wordt gezet, zijn de koppelingen gelegd, is de massale dataverwerking een feit en het systeem zal nooit onder controle zijn. Het gebruik van artificiële intelligentie voor *money control* zonder de nodige waarborgen zal tot duizenden dossiers leiden waar burgers onterecht beschuldigd zullen worden. Dit is niet hoe een volwassen democratie met grondrechten hoort om te gaan.

Chat control 2.0 is vandaag omgeven door een waaier aan vraagtekens. De eerste versie 1.0 is dankzij scherpe juridische adviezen en massaal burgerprotest verdwenen, maar het Deense voorzitterschap, dus de socialisten van Denemarken, werkt nu aan een zachte versie waarbij de “*detection orders*” op papier verdwijnen, maar in de praktijk via de risicobeperkende maatregelen kunnen terugkeren.

De concrete tekst van *chat control 2.0* is vooral gekend dankzij lekken van gespecialiseerde media, maar niet dankzij openbaarheid van bestuur. Hetzelfde geldt voor dit verhaal: over de DAM-fiches bestaat er veel onduidelijkheid.

Une proposition de loi de Vanessa Matz, Maxime Prevot (Les Engagés), Georges Dallemagne (Les Engagés) et Catherine Foncq (cdH) avait été déposée afin d’obtenir plus de transparence sur les fiches DAM. Par le biais de cette proposition, les fiches DAM devaient être dévoilées dans le cadre de la loi du 11 avril 1994 relative à la publicité de l’administration.

L’idée d’apporter plus de transparence dans ces fiches était une bonne idée, mais elle n’a pas pu aboutir avec la coalition Arizona.

Voorts benadrukt de heer Van Quickenborne dat dit dossier een dermate inbreuk op de privacy van mensen vormt, dat dit door gewone parlementsleden niet kan worden gesteund. Maar denken dat publiek protest zal wegblijven is een illusie.

Hoe langer dit debat plaatsvindt, hoe meer mensen zich gaan beginnen roeren. Om dit te illustreren verwijst hij naar een post op de sociale media van Matthias Dobbelaere-Welvaart, directeur van Ministry of Privacy en grote verdediger van onze privacy waarin hij zegt dat *money control* niet zal misstaan in andere totalitaire regimes.

Verder onderstreept de heer Dobbelaere-Welvaart dat er momenteel in de regering en in de commissie druk

Les citoyens ne s’intéresseront à *money control* qu’une fois que le système aura été instauré et voté, et il ne sera jamais supprimé. Si la machine algorithmique est lancée et que des recoupements ont été établis, le traitement massif des données sera devenu une réalité et le système échappera à tout contrôle. Utiliser l’intelligence artificielle dans le cadre de *money control* sans prévoir les garanties nécessaires débouchera sur des milliers de dossiers où des citoyens seront injustement accusés. Ce n’est pas ainsi qu’une démocratie adulte et respectueuse des droits fondamentaux devrait fonctionner.

Chat control 2.0 soulève aujourd’hui de nombreuses questions. Sa version 1.0 a disparu grâce à des avis juridiques pointus et à une contestation citoyenne massive, mais la présidence danoise, c’est-à-dire les socialistes danois, travaille actuellement à une version édulcorée dans laquelle les “ordres de détection” auront disparu sur papier, mais pourront faire leur réapparition en pratique au travers des mesures de réduction des risques.

On connaît surtout le contenu du texte de *chat control 2.0* grâce aux fuites intervenues dans des médias spécialisés, et non grâce à la publicité de l’administration. Il en va de même pour le dossier à l’examen: les fiches DAM suscitent de nombreuses interrogations.

Une proposition de loi de Vanessa Matz, Maxime Prevot (Les Engagés), Georges Dallemagne (Les Engagés) et Catherine Fonck (Les Engagés) avait été présentée afin d’obtenir plus de transparence sur les fiches DAM. Par le biais de cette proposition, les fiches DAM devaient être dévoilées dans le cadre de la loi du 11 avril 1994 relative à la publicité de l’administration.

L’idée d’apporter plus de transparence dans ces fiches était une bonne idée, mais elle n’a pas pu aboutir avec la coalition Arizona.

M. Van Quickenborne poursuit en soulignant que le projet à l’examen porterait une telle atteinte à la vie privée des citoyens qu’il ne peut pas être soutenu par des parlementaires ordinaires. Il serait toutefois illusoire de croire qu’aucune contestation populaire n’éclatera.

Plus ce débat se prolongera, plus les personnes qui commenceront à s’opposer au projet seront nombreuses. Pour illustrer son propos, l’intervenant renvoie à une publication postée sur les réseaux sociaux par Matthias Dobbelaere-Welvaart, directeur de l’association Ministry of Privacy et grand défenseur de notre vie privée, dans laquelle celui-ci indique que *money control* aurait sa place dans d’autres régimes totalitaires.

M. Dobbelaere-Welvaart indique aussi que d’intenses discussions sont actuellement menées au sein

wordt besproken over het feit dat de fiscus alle rekeningen, saldi en contracten wil samenvoegen in één grote databank, waarop men artificiële intelligentie wil loslaten. Hij voegt er ook aan toe dat wat er nu op tafel ligt nog verregaander is, namelijk een massieve databank van alle bezittingen van alle Belgen. Vermoeden van fraude is niet meer nodig. Het enige wat nodig zal zijn om iemand te verdenken als fraudeur is een AI-belletje.

Volgens de heer Van Quickenborne is het debat dus in gang geschoten en zal het gevoerd worden totdat iedereen weet waarover het gaat en daar een mening over heeft.

En het debat mag pas stoppen als iedereen zegt of hij voor of tegen is, in alle eerlijkheid en in alle transparantie. Mocht de spreker dit debat niet gevoerd hebben, de meerderheid van het Parlement had zelfs niet geweten waarover het ging. Dat debat is dus nodig en het is de taak van het Parlement om te zeggen wat er staat te gebeuren en om de mensen in te lichten.

Voorts legt de spreker de nadruk op het feit dat tot voor enkele maanden geleden er niet over *chat control* werd gesproken omdat het verhuld werd als een technisch voorstel. Het is een kwestie van proportionaliteit, transparantie en de vraag is ook of we ons in dit land alles kunnen permitteren. Het is niet omdat iets technologisch kan, dat het mag.

Artificiële intelligentie is een fantastisch instrument, maar het kan ook dingen beweren die totaal onjuist zijn. En als AI als tool wordt gebruikt op al de bankgegevens, dan moeten wij ons zorgen maken. Het is niet dat de liberalen tegen technologie zijn. Maar voor de vooruitgang zijn is iets anders dan alle overheidsbemoeienissen aanvaarden. En dat is de reden van dit debat.

De Belgische regering zit mee aan de tafel in de Raad waar over de teksten *chat control 2.0* wordt onderhandeld. Welke positie neemt daar de regering aan? De regering moet duidelijk maken dat België niet zal meewerken aan een systeem van verkapte massasurveillance en consequent zijn in dit parlement. Als de minister vindt dat *chat control* een brug te ver is, moeten we in elk geval twee keer nadenken vooraleer we *money control* invoeren.

De heer Van Quickenborne sluit dit punt af door te benadrukken dat burgerprotest in Europa bewezen heeft

du gouvernement et de la commission à propos du fait que l'administration fiscale souhaite rassembler tous les comptes, soldes et contrats au sein d'une grande base de données unique, qu'il souhaite ensuite soumettre à une analyse reposant sur l'intelligence artificielle. Il ajoute que le projet de loi à l'examen va encore plus loin, puisqu'il vise à créer une gigantesque banque de données comprenant l'ensemble des avoirs de tous les Belges. Des suspicions de fraude ne seront plus nécessaires: une alerte générée par intelligence artificielle suffira pour soupçonner un individu de fraude.

Selon M. Van Quickenborne, le débat a donc été lancé, et il sera mené jusqu'à ce que chaque citoyen connaisse la portée du projet à l'examen et qu'il se soit forgé un avis.

Et ce débat ne pourra s'arrêter que lorsque chacun dira s'il est pour ou contre le projet, en toute honnêteté et en toute transparence. Si l'intervenant n'avait pas mené ce débat, la majorité n'aurait même pas su de quoi il en retournait. Ce débat est donc nécessaire, et il appartient au parlement d'expliquer ce qui est sur le point d'arriver et d'informer la population.

L'intervenant souligne en outre que, jusqu'à il y a quelques mois, *chat control* ne faisait l'objet d'aucun débat, étant donné que ce projet était présenté comme une proposition de nature technique. C'est une question de proportionnalité, de transparence, et la question est aussi de savoir si nous pouvons tout nous permettre dans ce pays. La possibilité, sur le plan technologique, de mettre en œuvre une mesure ne justifie pas de l'autoriser.

L'intelligence artificielle est un outil formidable, mais elle peut également formuler des affirmations totalement fausses. Et si l'intelligence artificielle est utilisée comme outil d'analyse de toutes les données bancaires, il y a lieu de s'inquiéter. Ce n'est pas que les libéraux soient opposés à la technologie, mais il y a une différence entre le fait d'être favorable au progrès et le fait d'accepter toutes les ingérences des autorités. Telle est la raison de ce débat.

Le gouvernement belge participe aux négociations du Conseil sur les textes relatifs à *chat control 2.0*. Quelle est la position du gouvernement en la matière? Le gouvernement doit y indiquer clairement que la Belgique ne coopérera pas à un système de surveillance de masse déguisée, et agir conformément à cette position au sein de ce parlement. Si le ministre estime que *chat control* va trop loin, il nous faudrait alors réfléchir à deux fois avant d'instaurer *money control*.

M. Van Quickenborne conclut ce point en soulignant que les contestations citoyennes en Europe ont démontré

dat het massasurveillance kan terugdringen zolang er transparantie en tijd voor debat is. België moet dus wetgeving maken die dat soort democratische tegenkracht niet onmogelijk maakt, maar juist mogelijk.

Dat is de reden waarom de spreker dit debat hier voer en waarom hij de vergelijking heeft gemaakt met *chat control 1.0*, *Chat-Control 2.0* en *money control*.

De heer Lode Vereeck (VB) merkt op dat *money control* niet los kan gezien worden van een aantal andere gelijkaardige evoluties in onze samenleving. De bedoeling van zijn tussenkomst is om de minister duidelijk te maken in welk groot spel hij eigenlijk meespeelt. Dit gaat immers niet alleen over *money control*, dit gaat echt over het optuigen van een controlestaat.

In zijn betoog legt de spreker telkens de link tussen *chat control* en *money control* om de minister aan te geven wat hij daaruit kan leren en hoe dat hij dit grote fiasco kan vermijden. Het debat over *Invoice Control* dat eraan zit te komen bijvoorbeeld houdt rechtstreeks verband met *money control*.

De eerste tussenkomst van de heer Vereeck op *money control* was op 18 maart in de commissie Financiën naar aanleiding van de beleidsverklaring Financiën. Toen heerste het gevoel in de commissie dat daar een draak van wetgeving op ons afkwam. Toen al werden de eerste kritieken voorzichtig geformuleerd.

Op 2 juni is in de commissie Financiën de programwet voor het eerst besproken. Zowel bij de commissiebespreking als in de plenaire vergadering heeft de spreker zijn bezorgdheden duidelijk gemaakt. En die waren eigenlijk vooral geconcentreerd op het opheffen van het vermoeden van onschuld, een fundamentele pijler in onze rechtsstaat.

Ondertussen is mede dankzij collega Van Quickenborne duidelijk geworden dat er veel meer aan de hand was dan het gewoon vernietigen van het vermoeden van onschuld.

Money control: wat staat er op het spel?

Er wordt vaak gezegd dat de socialisten, de partij Vooruit, absoluut eisende partij zijn voor dit systeem. De spreker hoopt hen dus te overtuigen over de bias die in allerlei manieren van datamining zit.

Het is belangrijk om te begrijpen hoe datamining en de selectieprocedures werken en om te beseffen

qu'il est possible de faire reculer la surveillance de masse tant qu'il y a de la transparence et du temps pour le débat. La Belgique doit donc élaborer une législation qui ne neutralise pas ce type de contre-pouvoir démocratique, mais qui permette au contraire de l'exercer.

C'est pourquoi l'intervenant mène ce débat ici et pourquoi il a établi une comparaison entre *chat control 1.0*, *chat control 2.0* et *money control*.

M. Lode Vereeck (VB) relève que *money control* ne peut être considéré isolément de plusieurs autres évolutions similaires dans notre société. L'objectif de son intervention est de permettre au ministre de se rendre compte de la situation globale dans laquelle ses mesures s'inscrivent. Il ne s'agit en effet pas seulement de *money control*, mais bien de la mise en place d'un État contrôleur.

Dans son exposé, l'intervenant établit à chaque fois le lien entre *chat control* et *money control* afin d'indiquer au ministre ce qu'il peut en tirer comme enseignement et comment il peut éviter que *money control* débouche lui aussi sur un véritable fiasco. Le débat relatif à *Invoice Control*, qui va être mis en place, est par exemple en lien direct avec *money control*.

La première intervention de M. Vereeck sur *money control* a eu lieu le 18 mars en commission des Finances, à l'occasion de l'exposé d'orientation politique Finances. À ce moment, la commission était animée par le sentiment qu'une législation effrayante était en préparation. De premières critiques prudentes ont alors été formulées.

Le 2 juin, la loi-programme a été discutée pour la première fois en commission des Finances. Tant lors de la discussion en commission qu'en séance plénière, l'intervenant a exprimé clairement ses préoccupations. Celles-ci portaient en fait principalement sur la suppression de la présomption d'innocence, pilier fondamental de notre État de droit.

Entre-temps, grâce notamment à son collègue M. Van Quickenborne, il est apparu que les mesures prévues n'auraient pas seulement pour effet de supprimer la présomption d'innocence.

Money control: quel est l'enjeu?

Il est souvent affirmé que ce sont les socialistes du parti Vooruit qui réclament à cor et à cri la mise en place de ce système. L'intervenant espère donc les convaincre des biais qui affectent l'exploration des données de différentes manières.

Il est important de comprendre comment fonctionnent l'exploration de données et les procédures de sélection

dat zoiets bestaat als kenmerkbias of proxybias. Stel dat in *money control* in het CAP, een van de gebruikte parameters in het algoritme de postcode zou zijn. Dan zouden niet zozeer de rijke burgers, maar evengoed onze armere medeburgers kunnen geselecteerd worden door dit systeem.

De heer Vereeck legt dus de nadruk op algoritmische bias in het systeem, d.w.z. een vertekening of vooringenomenheid of vooroordelen, die natuurlijk niet zichtbaar is. Het gaat niet over flagrante discriminatie omdat alles ingekapseld zit in een dataminingmodel. Maar het bestaat wel.

Het is dus te hopen dat de linkse partijen, in het bijzonder Vooruit, in de commissie Financiën toch eens even aan de mouw trekken bij hun partij om duidelijk te maken dat de algoritmes vertekend kunnen zijn met een bepaalde bias. Dit kan bijvoorbeeld het geval zijn als men werkt op basis van een postcode. De algoritmes werken ook op historische leerprocessen. Als men merkt dat iemand al in aanmerking is gekomen voor fiscale fraude of voor sociale fraude – want in het regeerakkoord staat ook dat al die databanken gekoppeld zullen worden, zowel die van de FOD Financiën als de Sociale Zekerheid, dus men is niet alleen op zoek naar fiscale fraude, maar ook naar sociale fraude – dan zou het wel kunnen dat wat een neutraal zoekcriterium lijkt, eigenlijk een proxy is voor sociaaleconomische segregatie. Dat geldt trouwens ook voor andere selectiecriteria, zoals al dan niet een zelfstandige activiteit uitoefenen, de sector waar men werkt waar er misschien al sprake van fraude is geweest in het verleden of het opleidingsniveau.

Dit om te tonen dat ook andere problemen zoals modelbias, evaluatiebias, databronbias, zich kunnen stellen. De spreker komt daar later nog op terug, maar wil dat de collega's van Vooruit goed nadenken of *money control* wel de manier is waarop zij willen verder gaan om fiscale fraude tegen te gaan.

De heer Vereeck buigt zich vervolgens over *chat control* en de beleidslogica achter de EU-verordening. Het doel van deze regelgeving bestaat erin om bepaalde mensen – namelijk de minderjarigen – in een gedigitaliseerde samenleving te beschermen, meer bepaald tegen seksueel misbruik.

Het volume van online kindermisbruik neemt exponentieel toe. De spreker verwijst in dit verband naar de RIA (*Regulatory Impact Assessment*) over seksueel kindermisbruik in de Europese Unie. Ook al is het naar

pour réaliser qu'elles peuvent présenter des biais d'agrégation ou des biais de proxy. Supposons qu'au sein du PCC, l'un des paramètres utilisés par l'algorithme de *money control* soit le code postal. Dans ce cas, nos concitoyens moins aisés pourraient tout autant être sélectionnés par ce système que les citoyens riches.

M. Vereeck met donc l'accent sur le biais algorithmique qui affecte le système, lorsque l'algorithme est basé sur une distorsion, une partialité ou des préjugés, qui ne sont évidemment pas visibles. Il ne s'agit pas d'une discrimination flagrante puisque celle-ci est entièrement enveloppée dans un modèle de *data mining*. Mais elle existe bel et bien.

Il est donc à espérer que les membres des partis de gauche représentés en commission des Finances, en particulier Vooruit, interpellent leur formation afin de lui montrer que les algorithmes peuvent être faussés par un biais déterminé. Celui-ci peut par exemple apparaître lorsque le code postal est intégré à l'algorithme. Les algorithmes reposent par ailleurs sur des processus d'apprentissage historiques. S'il est constaté qu'une personne a déjà été associée à un cas de fraude fiscale ou de fraude sociale – l'accord de gouvernement prévoit en effet que les banques de données du SPF Finances et de la Sécurité sociale seront interconnectées, de sorte que le but ne sera pas seulement de repérer des cas de fraude fiscale mais aussi de fraude sociale –, il se pourrait qu'un critère de recherche apparemment neutre constitue en réalité un proxy de ségrégation socio-économique. Cela vaut d'ailleurs aussi pour d'autres critères de sélection, tels que l'exercice ou non d'une activité indépendante, le secteur d'activité – surtout si des cas de fraude y ont été repérés par le passé – ou encore le niveau de formation.

Il ressort de ce qui précède que d'autres problèmes, tels que le biais de modèle, le biais d'évaluation ou le biais lié aux sources de données utilisées, sont également susceptibles de se poser. L'intervenant y reviendra plus tard, mais souhaite que les collègues de Vooruit se demandent sérieusement si *money control* est bien la voie qu'ils veulent suivre pour lutter contre la fraude fiscale.

M. Vereeck se penche ensuite sur *chat control* et la logique politique qui sous-tend le règlement européen. L'objectif de cette réglementation est de protéger certaines personnes – à savoir les mineurs – dans notre société numérisée, plus particulièrement contre les abus sexuels.

Le volume des maltraitances d'enfants en ligne augmente de manière exponentielle. L'intervenant renvoie à cet égard à l'analyse d'impact de la réglementation (AIR) concernant les abus sexuels d'enfants dans l'Union

zijn mening geen goede RIA, toch heeft het de verdienste om in te schatten waarover men het heeft. De vraag is immers altijd of de wetgeving wel noodzakelijk is? Als het om een beperkt aantal casussen gaat, dan is dat niet het geval. Wat *chat control* betreft is het dus duidelijk dat die wetgeving wel zin heeft.

Wat fiscale fraude betreft is het echter een andere zaak. In zijn rapport heeft de Nederlandse Wetenschappelijke Raad voor het Regeringsbeleid de problemen voor *big data* analyse en de fundamentele rechten van mensen onderzocht.

In hoofdstuk vier van dat rapport, dat specifiek over fiscaliteit gaat, geeft men een overzicht van de ramingen van fiscale fraude. Het is altijd goed om aan te geven wat de omvang is van de fiscale fraude die u wil behandelen.

Het is niet dat fiscale fraude in belastingaangifte verwaarloosbaar is in België, maar stel dat fiscale fraude bij de btw-aangifte vele malen groter is, dan is het misschien nuttiger om zich toe te spitsen op de strijd tegen de btw-fraude, in plaats van ons bezig te houden met *money control*.

Te noteren valt dat een recent rapport van de Europese Commissie ons land aan de top van de btw-niet-naleving plaatst. De btw-kloof wordt op euro 4,5 miljard geschat. Dat is misschien een tip voor minister Jambon: de btw-kloof met de helft terugbrengen – op het Europese gemiddelde – zou meteen 2,5 miljard opbrengen.

Dit is dus een eerste opmerking van de spreker: voor *chat control* is er een duidelijk zicht op de omvang van de problematiek. Hier wordt dat zelfs nog niet gesuggereerd. Het idee is dat we tegen fiscale fraude moeten zijn omdat het zo is.

Ten tweede, het is duidelijk dat wat *chat control* betreft, de vrijwillige detectie en detectie door technologiebedrijven onvoldoende systematisch en betrouwbaar is. De fiscale kliklijnen bestaan wel, maar weinig burgers zullen op vrijwillige basis nog wat willen bijbetalen.

In *money control* ontbreekt die vrijwilligheid. De Commissie heeft dus een model naar voren geschoven die een verplichting invoert om actief en continu te scannen op signalen van misbruik.

européenne. Même si, selon lui, la qualité de cette AIR laisse à désirer, elle a néanmoins le mérite de permettre une approche adéquate de la problématique. La question est en effet toujours de savoir si une réglementation est nécessaire. Elle ne l'est pas si le nombre de situations visées est limité.

En ce qui concerne la fraude fiscale, le Conseil scientifique néerlandais pour la politique gouvernementale a, dans son rapport, examiné les problèmes liés à l'analyse des mégadonnées et aux droits fondamentaux des personnes.

Le chapitre 4 de ce rapport, qui porte spécifiquement sur la fiscalité, donne une estimation de l'ampleur de la fraude fiscale, ce qui est toujours utile quand l'intention est de lutter contre celle-ci.

L'intervenant ne considère pas que l'ampleur de la fraude fiscale dans les déclarations d'impôt est négligeable en Belgique mais, à supposer que la fraude fiscale dans les déclarations de TVA soit beaucoup plus importante, il serait peut-être plus utile de se concentrer sur la lutte contre la fraude à la TVA au lieu d'instaurer *money control*.

Il convient de noter qu'un rapport récent de la Commission européenne place notre pays en tête du non-respect des règles en matière de TVA. Le déficit de TVA est estimé à 4,5 milliards d'euros. Un conseil à adresser au ministre Jambon pourrait être de réduire de moitié le déficit de TVA – pour le ramener à la moyenne européenne –, ce qui rapporterait immédiatement 2,5 milliards.

La première observation de l'intervenant est donc qu'en ce qui concerne *chat control*, l'ampleur de la problématique apparaît clairement, tandis qu'au sujet de *money control*, elle n'est même pas évoquée. Le postulat de départ est qu'il y a lieu de combattre la fraude fiscale parce qu'il doit en être ainsi.

Deuxièmement, il est clair qu'en ce qui concerne *chat control*, la détection volontaire et la détection par les entreprises technologiques ne sont pas suffisamment systématiques et fiables. En matière fiscale, il existe des canaux de dénonciation mais peu de citoyens voudront payer volontairement davantage d'impôt.

Le caractère volontaire fait défaut en ce qui concerne *chat control*. La Commission a donc présenté un modèle qui introduit une obligation de scanner activement et en continu les signaux d'abus.

Dit kan bijna een-op-een gekopieerd worden voor *money control*: er zal een systeem komen dat actief en continu zal scannen op belastingrisicogedrag.

De spreker vestigt de aandacht op het feit dat de wetgeving in een amendement zou moeten opnemen dat het hier gaat over de bestrijding van fiscaal fraudegedrag. D.w.z. alle handelingen of patronen die de kans vergroten dat een persoon al dan niet opzettelijk in overtreding is met de fiscale wetgeving. Het is dus een veel breder begrip dan belastingfraude. Belastingfraude is opzettelijk. Belastingrisicogedrag kan per ongeluk zijn.

Voorbeelden van bekend risicogedrag zijn onder andere de optimalisatie van uw belastingplanning. Als dat ook hoort tot het opstellen van risicoprofielen in *money control*, betekent dat dat een hele sector in de brandhaard wordt gegooid terwijl er nog altijd niets mis is met de optimalisering van uw belasting.

De heer Van Quickenborne komt even tussen op het punt van de belastingoptimalisatie.

In deze commissie is er een wetsvoorstel van Vooruit geweest waarin over optimalisatie om in geval van overlijden bij een koppel de juiste en meest voordelige fiscale aangifte te doen. De spreker was bereid om dit wetsvoorstel te steunen op voorwaarde dat dit alle vormen van optimalisatie zou betreffen. Als fiscale optimalisatie nu het voorwerp van *money control* wordt, dan zal het systeem nog erger zijn dan datgene wat hij had voorspeld. De vraag van meneer Vereeck over risicogedrag is dus zeker pertinent.

De heer Vereeck wijst erop dat rekening houdend met de manier waarop *money control* vandaag omschreven is, risicogedrag ook zou worden onderzocht. Zelfs een boete, het overtreden van een regel kan aanleiding zijn om door het algoritmische model te worden geselecteerd. Het kan gaan van slechte administratie tot het niet documenteren van inkomsten. Ook een inconsistente of te late aangifte en wat men noemt risicovolle zakelijke praktijken behoren tot risicogedrag. Bijvoorbeeld actief zijn in sectoren waar veel cash geld wordt gebruikt.

In dit verband merkt de spreker op dat de sectoren die veel cash geld gebruiken waarschijnlijk geen sectoren zijn waar men over enorme bedragen spreekt. Het zou dus kunnen gaan over sectoren waar laaggeschoolde

Ce constat peut presque être transposé tel quel s'agissant de *money control*: un système scannera activement et en continu les comportements à risque en matière fiscale.

L'intervenant attire l'attention sur le fait que le législateur devrait préciser dans un amendement que l'objectif est de lutter contre les comportements à risque sur le plan fiscal, c'est-à-dire tous les actes ou comportements qui augmentent le risque qu'une personne enfreigne, intentionnellement ou non, la législation fiscale. Il s'agit donc d'une notion nettement plus large que celle de la fraude fiscale. La fraude fiscale est intentionnelle. Les comportements à risque sur le plan fiscal peuvent être involontaires.

L'optimisation de la planification fiscale est un exemple de comportement à risque connu. Si cela donne également lieu à l'établissement de profils à risque dans *money control*, tout un secteur sera mis en péril, alors que l'optimisation fiscale ne constitue pas, en soi, une infraction.

M. Van Quickenborne intervient brièvement sur le sujet de l'optimisation fiscale.

Cette commission a examiné une proposition de loi du groupe Vooruit visant à optimiser la déclaration fiscale d'un couple en cas de décès de l'un des conjoints afin que la déclaration soit la plus correcte et la plus avantageuse possible. L'intervenant était disposé à soutenir ce projet de loi à condition qu'il concerne toutes les formes d'optimisation. Si l'optimisation fiscale devient maintenant la cible du *money control*, le système sera encore pire que ce qu'il avait prédit. La question de M. Vereeck sur les comportements à risque est donc totalement pertinente.

M. Vereeck indique qu'il se déduit de la description actuelle du *money control* que les comportements à risque seraient également examinés. Même une simple amende ou la violation d'une règle pourra donner lieu à une sélection par le modèle algorithmique. Le membre cite d'autres exemples de comportements à risque: une mauvaise administration, l'absence de justification de certains revenus, l'incohérence ou le dépôt tardif d'une déclaration ou encore ce que l'on appelle des pratiques commerciales à risque, par exemple être actif dans des secteurs où beaucoup d'espèces circulent.

À cet égard, l'intervenant fait observer que les secteurs où beaucoup d'espèces circulent ne sont probablement pas des secteurs qui brassent des sommes colossales. Cela pourrait donc concerner des secteurs qui occupent

mensen zitten, die misschien cash worden uitbetaald door hun werkgever en dat geld op hun rekening te zetten.

De heer Van Quickenborne sluit zich aan bij de heer Vereeck. De verantwoording bij de amendementen verwijst naar ernstige en georganiseerde belastingfraude, btw-carroussels, domiciliëfraude, offshoreconstructies, en naar indiciaire tekorten. In zijn verantwoording neemt de minister het voorbeeld van de foorkramers als sector met veel kleine cash transacties. Die worden dus het doelwit van *money control*. Dit is ver af van de ernstige georganiseerde fraude.

De heer Vereeck wijst erop dat gewone mensen – de foorkramers, marktkramers – dus ook gevisieerd worden. Het verschil tussen de uitgaven en de inkomsten van een persoon werd vroeger ook al door de fiscus via dataminingtechnieken gedetecteerd. Daar is geen *money control* voor nodig. Als er al een vermoeden van fraude was, dan was de fiscus naar het CAP gegaan en had die toegang gevraagd de financiële data.

Belastingrisicogedrag kan ook het resultaat zijn van een onjuist begrip van belastingplichtigen. In dit verband is er in deze commissie een uitgebreide discussie geweest over de *carried interest*, waarbij de vraag was of het inkomen van een vermogensfondsbeheerder, een beroeps- of vermogensinkomen is.

Waarom wordt de term belastingrisico gebruikt?

Zoals omschreven in de literatuur en in de tekst van de minister wordt belastingrisico gebruikt om patronen te identificeren. Het is een probabilistisch model die de kans moet inschatten dat een belastingplichtige niet door een controle komt. Het gaat er dus zelfs niet over fraude plegen, het gaat er over dat men denkt dat iemand niet slim genoeg is om door een belastingcontrole te geraken. Dat is zeer ondemocratisch.

Het dient ook om allerlei interventies te sturen, zoals herinneringen, voorlichting of controles. De Belgische fiscus doet in dat kader aan "*nudging*". Het grote verschil hier is dat het op macroschaal zal gebeuren. Dus niet meer op basis individuele rekeningen.

Belastingsrisicogedrag is interessant in de zin dat als het consequent wordt toegepast, het mogelijk is om een onderscheid maken tussen oprechte fouten

des travailleurs peu qualifiés, qui sont peut-être payés en espèces par leur employeur et qui déposent cet argent sur leur compte.

M. Van Quickenborne rejoint M. Vereeck. La justification des amendements évoque la fraude fiscale grave et organisée, les carrousels à la TVA, la fraude au domicile, les montages offshore et les déficits indiciaires. Dans sa justification, le ministre prend les forains comme exemple de secteur où les petites transactions en espèces sont nombreuses. Ceux-ci deviendront donc la cible du *money control*. Il n'est pourtant absolument pas question, dans leur cas, de fraude grave et organisée.

M. Vereeck souligne que des citoyens ordinaires comme les forains ou les commerçants ambulants seront donc également visés. La différence entre les dépenses et les revenus d'une personne était déjà détectée auparavant par l'administration fiscale grâce à des techniques de *data mining*. Il n'est pas nécessaire de recourir au *money control* à cette fin. En cas de suspicion de fraude, le fisc s'adressait au PCC pour demander l'accès aux données financières.

Les comportements à risque sur le plan fiscal peuvent également découler d'une mauvaise compréhension de la part des contribuables. À cet égard, cette commission a mené une discussion approfondie sur l'intéressement aux plus-values, afin de déterminer si les revenus d'un gestionnaire de fonds d'investissement constituaient des revenus professionnels ou des revenus patrimoniaux.

Pourquoi le terme "risque fiscal" est-il employé?

Comme décrit dans la littérature et dans le texte du ministre, le risque fiscal est utilisé pour identifier des schémas. Il s'agit d'un modèle probabiliste qui vise à évaluer la probabilité qu'un contribuable soit recalé en cas de contrôle. Il ne s'agit donc même pas d'identifier un contribuable qui se serait rendu coupable d'une fraude, mais plutôt de penser qu'un contribuable n'est pas assez malin pour passer un contrôle fiscal. C'est très antidémocratique.

Ce modèle sert également à orienter toutes sortes d'interventions, telles que des rappels, des demandes de renseignements ou des contrôles. Dans ce cadre, le fisc belge pratique le "*nudging*". La grande différence est que cela se fera en l'espèce à l'échelle macro et donc plus sur la base de comptes individuels.

La notion de comportement à risque sur le plan fiscal est intéressante dans le sens où, si elle est appliquée de manière cohérente, elle permettra d'opérer la distinction

en opzettelijke ontduiking en dat zou al een belangrijke eerste inperking zijn van *money control*.

Voorts onderstreept de spreker dat het feit dat enkel grootschalige datamining nog een afdoende oplossing zou bieden voor al die lekken in de begroting absurd is. Net zoals *chat control* steunt *money control* ook op de veronderstelling dat de traditionele opsporingsmethoden te kort schieten, maar niets is minder waar. De traditionele opsporingsmethoden worden in vraag gesteld en de digitale benadering, de algoritmische screening van de volledige populatie zou dus gerechtvaardigd zijn.

Zowel *chat control* als *money control* vertrekken vanuit een vergelijkbare, beleidsmatige probleemdefinitie die massale dataverwerking normaliseert. In dit verband werkt de heer Vereeck momenteel aan een RIA (*regulatory impact analysis*) en het eerste element om een RIA te maken is de probleemdefinitie is.

Wat is het probleem?

Het probleem onderscheidt zich in twee luiken. Het eerste luik betreft de cijfers en de vraag of het de moeite om daar regelgeving op los te laten.

Het tweede punt is de probleemdefinitie.

De spreker geeft hier een voorbeeld om te tonen hoe die probleemdefinitie automatisch tot een bepaalde regelgevingsoptie leidt. Als u bedelarij beschouwt als een sociaaleconomisch probleem, zult u cijfers geven met de achtergrond van bedelaars. Als u daarin een probleem van verstoring van de openbare orde ziet, dan gaat u een hele andere regelgeving naar voren schuiven.

Het is hetzelfde met *money control*. Als u begint met te zeggen dat er te veel fraude is, vooral financiële fraude – terwijl het wel eens btw-fraude zou kunnen zijn – en als u vervolgens suggereert dat de traditionele methodes ouderwets zijn, zorgt deze archaïsche manier om de zaken voor te stellen ervoor dat we moeten digitaliseren.

Chat control en de Europese context

De ontwikkeling van *chat control* moet begrepen worden in het veel bredere traject van de Europese regelgeving inzake digitale opsporing. Vanaf de data-retentierichtlijn in 2006 werd voor het eerst een systeem ingevoerd waarbij telecomproviders systematisch metadata van alle burgers moesten bewaren.

entre les erreurs sincères et la fraude délibérée, ce qui constituerait déjà une première restriction importante du *money control*.

En outre, l'intervenant souligne qu'il est absurde de penser que seul le *data mining* à grande échelle pourrait encore combler tous les trous dans le budget. À l'instar du *chat control*, le *money control* repose sur l'hypothèse que les méthodes de recherche traditionnelles ne sont pas suffisamment efficaces, mais rien n'est moins vrai. Les doutes concernant les méthodes de recherche traditionnelles justifieraient donc l'approche numérique, à savoir le screening algorithmique de l'ensemble de la population.

Tant le *chat control* que le *money control* partent d'une définition politique similaire du problème, qui normalise le traitement massif des données. Dans ce contexte, M. Vereeck prépare actuellement une AIR (analyse d'impact de la réglementation) et la première étape de cette analyse est la définition du problème.

Quel est le problème?

Le problème comporte deux volets. Le premier concerne les chiffres et la question de savoir si cela vaut la peine de réglementer en la matière.

Le deuxième point est la définition du problème.

L'intervenant donne un exemple visant à démontrer que la manière dont le problème est défini entraîne automatiquement une option réglementaire déterminée. Si on considère la mendicité comme un problème socioéconomique, on fournira des chiffres basés sur la situation des mendiants. Si, au contraire, on considère la mendicité comme un trouble à l'ordre public, on proposera une réglementation fondamentalement différente.

Il en va de même pour le *money control*. Si on part du postulat que la fraude, et en particulier la fraude financière – alors qu'il pourrait bien s'agir de la fraude à la TVA – est trop fréquente, et que l'on suggère ensuite que les méthodes traditionnelles sont désuètes, cette façon archaïque de présenter les choses nous contraint à passer au numérique.

Chat control et contexte européen

Le développement de *chat control* doit être situé dans le cadre beaucoup plus large de la réglementation européenne en matière de détection numérique. À partir de la directive sur la conservation des données de 2006, un système obligeant les opérateurs de télécommunications à conserver systématiquement les métadonnées de tous les citoyens a été mis en place pour la première fois.

Ook hier gaat het dus om het systematisch bewaren van alle financiële gegevens van alle burgers. De vernietiging van deze richtlijn door het Hof van Justitie in 2014 vormde natuurlijk ook een juridische breuklijn. Er werd toen gepreciseerd dat algemene en ongerichte bewaring van gegevens onverenigbaar is met de fundamentele rechten van de Europese burgers.

En sindsdien zoekt de Europese Commissie occasioneel naar nieuwe instrumenten om digitale opsporing te versterken. *chat control* past binnen deze herpositionering en de Europese Commissie probeert dit te verkopen als preventieve risicodetectie. En zo is de cirkel rond: het gaat om risicodetectie, niet om fraude.

Chat control en de Belgische context

De Belgische fiscale context vertoont een parallelle evolutie. Eerdere systemen van gerichte fiscale controle, zoals een klassieke audit of informatievergaring op verzoek worden sluipend, stap voor stap aangevuld door ingrijpende systemen, zoals CAP-datamining, de datamining van de databank met alle financiële gegevens van de burgers.

Dit is niet langer informatievergadering op verzoek, maar gewoon een systematische, ongemotiveerde inkijk in al onze rekeningen. Het risico bestaat dat ook in België een juridisch grensverleggende praktijk ontstaat, waarbij een vorm van massale surveillance wordt ingevoerd onder het etiket van preventieve fraudebestrijding. Net zoals *chat control* preventie gebruikt om juridisch veel ruimer te gaan dan klassieke opsporing.

Zoals onderstreept door de heer Vereeck heeft dit systeem sociale en economische gevolgen. Wanneer de mensen constant gescreend worden, heeft dit op den duur een impact op hun gedrag. Alle burgers van dit land, ook de ondernemers, gaan schrik hebben om op een financieel en fiscaal innovatieve manier een bepaald maatschappelijk of commercieel investeringsproject uit te voeren. Dus is wat men noemt “*the chilling effect*”: men durft niet meer economisch productief te zijn uit schrik om fouten te maken.

Rol van de regering en het Parlement

Het hele beleidsproces rond *chat control* vertoont hele sterke institutionele spanningen. De manier waarop er met dit ontwerp geïnjougeerd is, toont ook aan dat er hier binnen deze meerderheid enorme spanningen aan het ontstaan zijn.

Dans ce cadre, il s'agit donc également de la conservation systématique de toutes les données de tous les citoyens. Il va de soi que l'annulation de cette directive par la Cour de justice de l'Union européenne en 2014 a marqué une rupture juridique. Il a alors été précisé que la conservation généralisée et non ciblée des données est incompatible avec les droits fondamentaux des citoyens européens.

Depuis lors, la Commission européenne recherche occasionnellement de nouveaux instruments pour renforcer la détection numérique. Le *chat control* s'inscrit dans ce repositionnement et la Commission européenne tente de le présenter comme étant un outil de détection préventive des risques. La boucle est ainsi bouclée: il s'agit de détecter des risques, et non une fraude.

Chat control et contexte belge

Le contexte fiscal belge présente une évolution parallèle. Les anciens systèmes de contrôle fiscal ciblé, tels que l'audit classique ou la collecte d'informations à la demande, sont progressivement et discrètement complétés par des systèmes invasifs tels que le *data mining* PCC, à savoir le *data mining* de la banque de données contenant toutes les informations financières des citoyens.

Il ne s'agira plus d'une collecte d'informations à la demande, mais tout simplement d'un accès systématique et non motivé à tous les comptes des citoyens. Le risque existe qu'une pratique juridiquement novatrice voie également le jour en Belgique, avec l'introduction d'une forme de surveillance massive sous le prétexte de la lutte préventive contre la fraude, tout comme le *chat control* invoque la prévention pour aller beaucoup plus loin, sur le plan juridique, que les enquêtes classiques.

Comme l'a souligné M. Vereeck, ce système aura des conséquences sociales et économiques. Lorsque les gens sont constamment surveillés, cela finit par se répercuter sur leur comportement. Tous les citoyens de ce pays, y compris les entrepreneurs, auront peur de concrétiser un projet d'investissement dans la société ou à titre commercial en innovant sur les plans financier et fiscal. Ce phénomène s'appelle “l'effet paralysant” (*chilling effect*). Il survient lorsque l'on n'ose plus être économiquement productif de peur de commettre des erreurs.

Rôle du gouvernement et du Parlement

Tout le processus politique concernant le *chat control* fait apparaître de très fortes tensions institutionnelles. Le parcours chaotique du projet de loi à l'examen montre également que d'énormes tensions sont en train de naître au sein de cette majorité.

Dit komt doordat de Europese Commissie op een dwingend en uniform model van scanning aandringt, maar het Europees parlement is sterk verdeeld. En dat zien we ook in het Belgisch parlement.

Sommige fracties zijn daar zeer mondig in. Dit is het geval van Open Vld, VB en de MR-fractie, althans in een eerste aanzet van Mathieu Michel, tegen zijn coalitiepartners in, en niet in het minst de eerste minister. Ondertussen is het duidelijk geworden dat ook de N-VA-fractie tegen *money control* is, maar dat er daar een oekaze ligt, niet zozeer van de fractieleider, zelfs niet van de minister van Financiën, maar van de eerste minister zelf.

In het Europees parlement zijn de meningen ook verdeeld. Sommige fracties benadrukken het absolute belang van fraudebestrijding, andere achten de vergaande inbreuken op privacy onaanvaardbaar.

Wat de heer Vereeck vooral stoort in deze problematiek is de verregaande inbreuk op het fundamentele vermoeden van onschuld.

Binnen de Raad heeft daar een debat over gewoed waarbij Duitsland, Oostenrijk en Nederland onder andere hebben ingezet op proportionaliteit.

Want dat is het gevaar: het niet-proportionele karakter van *chat control*.

Er zit dus een *chat control 2.0* aan te komen. De moraal van het verhaal is dat wanneer wij denken om deze zevenkoppige draak te doden, hij toch als een klein draakje op een andere manier terug verschijnt.

De heer Lode Vereeck (VB) merkt dat er inzake *money control* een zekere institutionele spanning bestaat tussen de uitvoerende macht, de controleautoriteiten en het Parlement. Hij betreurt dat de regering de noodzaak van datamining blijft verdedigen, terwijl de GBA net hamert op de disproportionele aard van de praktijk. De spreker is bovendien van mening dat het Grondwettelijk Hof het wetsontwerp weleens zou kunnen vernietigen. Het betreft namelijk een technologisch en juridisch complex onderwerp, waarover de debatten volgens hem zijn verzand in politieke platitudes omtrent fraudebestrijding.

De heer Vereeck stelt dat een van de meest controverse aspecten van *chat control* het systeem van de zogeheten detectiebevelen is. Dergelijke bevelen kunnen worden opgelegd aan alle diensten die digitale communicatie mogelijk maken: berichtenapps, e-maildiensten, gamingplatforms, sociale media met privéchatfunctie

Ces tensions découlent du fait que la Commission européenne insiste en faveur d'un modèle contraignant et uniforme de *scanning*, alors que le Parlement européen est très divisé. Et le même phénomène peut être observé au Parlement belge.

Certains groupes politiques s'expriment sans retenue à ce sujet. Ce fut le cas de l'Open Vld, du VB et du groupe MR, du moins lors d'une première tentative de Mathieu Michel, contre ses partenaires de coalition, notamment contre le premier ministre. Il est aujourd'hui clair que le groupe N-VA est également opposé au *money control*, mais qu'il fait l'objet d'un diktat, non pas de la part du chef de groupe, ni même du ministre des Finances, mais bien du premier ministre lui-même.

Au sein du Parlement européen, les avis sont également partagés. Certains groupes insistent sur l'importance absolue de la lutte contre la fraude, tandis que d'autres jugent que les atteintes graves à la vie privée sont inacceptables.

Ce qui dérange particulièrement M. Vereeck dans cette problématique, c'est l'atteinte grave au principe fondamental de la présomption d'innocence.

Un vif débat a fait rage à ce sujet au sein du Conseil, où l'Allemagne, l'Autriche et les Pays-Bas, entre autres, ont mis l'accent sur la proportionnalité.

C'est en effet là que se situe le danger, c'est-à-dire dans le caractère non proportionnel du *chat control*.

Un *chat control 2.0* est donc en préparation, la morale de l'histoire étant que lorsque nous pensons avoir tué ce dragon à sept têtes, il réapparaît sous une autre forme, sous les traits d'un tout petit dragon.

M. Lode Vereeck (VB) constate, dans le cadre de *money control*, une tension institutionnelle entre le pouvoir exécutif, les autorités de contrôle et le Parlement. L'orateur déplore que le gouvernement persiste à défendre la nécessité du *data mining*, malgré son caractère disproportionné souligné par l'APD. Le député considère en outre que le projet de loi à l'examen risque d'être annulé par la Cour constitutionnelle, en raison de débats technologiques et juridiques complexes qu'il juge réduits à de simples slogans politiques sur la lutte contre la fraude.

M. Vereeck indique que l'un des aspects les plus controversés de *chat control* est la structure dite des "ordres de détection". Ces ordres peuvent être imposés à tous les services facilitant la communication numérique: applications de messagerie, services de courriel, plateformes de jeux, réseaux sociaux avec messagerie

enzovoort. Volgens de spreker heeft *chat control* een nagenoeg universele reikwijdte, anders dan *money control*. Detectiebevelen verplichten dienstverleners evenwel om specifieke algoritmes in te bouwen, met name via bekende vormen van datamining.

Het lid betreurt bovendien dat de minister ontkent dat de FOD Financiën artificiële intelligentie zou gebruiken om zijn dataminingmodellen te ontwikkelen. De spreker onderstreept dat de belastingdiensten van talloze Europese landen AI gebruiken voor een op algoritmes gebaseerde fiscale controle. Voor de heer Vereeck is de toepassing van dergelijke modellen op de hele bevolking volstrekt uit den boze. Hij voegt eraan toe dat *money control* de nationale overheden een ongeziene machtspositie zou geven, omdat zij dan zouden bepalen welke detectiemodellen worden gebruikt en in welke mate ze worden toegepast. De spreker benadrukt dat de analogie met de uitbreiding van datamining overduidelijk is. Terwijl *chat control* universele detectie behelst via scanningbevelen, biedt *money control* de belastingadministratie de mogelijkheid om via het CAP elke financiële transactie tegen het licht te houden. Volgens de spreker verstoren dergelijke praktijken het evenwicht tussen staat en burger door gegevens standaard toegankelijk te maken, terwijl die gegevenstoegang net de uitzondering zou moeten blijven.

Hij vindt hoe dan ook dat dit debat in de juiste context moet worden geplaatst: die van de interne markt en de digitale soevereiniteit. De Europese Commissie heeft *chat control* net zoals *money control* uitdrukkelijk opgenomen in de logica van de interne markt. De spreker waarschuwt voor het risico dat consumenten in België strenger zouden worden gecontroleerd dan in andere lidstaten en zo hun koopkracht aangetast zouden zien. Hij pleit derhalve voor een eengemaakte regeling binnen de hele interne markt en meent dat voor alle in de EU actieve dienstverleners dezelfde verplichtingen zouden moeten gelden, ongeacht waar ze zijn gevestigd. Een dergelijke regeling zou passen in een bredere strategie voor digitale soevereiniteit.

De heer Vereeck wijst op een mogelijke tegenstrijdigheid: men vergroot de Europese digitale autonomie door systemen op te leggen die volgens sommige experts de digitale veiligheid zouden aantasten. Bedrijven vrezen dat de verplichting om scans uit te voeren hen weleens zou kunnen confronteren met een njet van andere rechtscolleges, waardoor naleving complex wordt en innovatie wordt belemmerd. Zeker in het kader van *money control* is een en ander aldus de spreker relevant: in de financiële en fiscale sector bestaat er namelijk een soortgelijke spanning. Volgens de heer Vereeck wil België zijn fiscale autonomie vergroten via een centraal systeem voor datamining, maar loopt het tegelijkertijd

privée, etc. Selon l'orateur, la portée de *chat control* est quasiment universelle, ce qui n'est pas le cas pour *money control*. Toutefois, les ordres de détection obligent les fournisseurs à implémenter des algorithmes spécifiques, notamment via des formes connues de *data mining*.

Par ailleurs, le membre déplore que le ministre ait nié que le SPF Finances utilise l'intelligence artificielle pour développer ses modèles de *data mining*. Il souligne que les administrations fiscales de plusieurs pays européens recourent à l'intelligence artificielle pour permettre un contrôle fiscal algorithmique. Dans ce contexte, M. Vereeck marque son opposition totale à l'application de ces modèles à l'ensemble de la population. Il ajoute que *money control* créerait une position de pouvoir inédite pour les autorités nationales, qui détermineraient quels modèles de détection sont utilisés et dans quelle mesure ils sont déployés. L'intervenant souligne que l'analogie avec l'expansion du *data mining* est évidente. Alors que *chat control* instaure une détection universelle via des ordres de scanning, *money control* ouvre la possibilité pour l'administration fiscale d'examiner toutes les transactions financières à partir du PCC. Selon lui, ces mécanismes déplacent l'équilibre entre le citoyen et l'État en institutionnalisant un accès standard aux données, là où cet accès devrait rester exceptionnel.

L'orateur insiste également sur la nécessité de replacer ce débat dans le cadre du marché intérieur et de la souveraineté numérique. La Commission européenne a expressément inscrit *chat control* dans la logique du marché intérieur, ce qui vaut aussi pour *money control*. Le député met en garde contre le risque que les consommateurs belges soient soumis à des contrôles plus stricts que dans d'autres États membres, ce qui pourrait affecter leur pouvoir d'achat. Il plaide dès lors pour une harmonisation au sein du marché intérieur et estime que tous les prestataires actifs dans l'Union européenne doivent donc être soumis aux mêmes obligations, quel que soit leur lieu d'établissement, ce qui s'inscrit dans une stratégie plus large de souveraineté numérique.

M. Vereeck soulève la question d'une possible contradiction: renforcer l'autonomie numérique européenne en imposant des systèmes qui, selon certains experts, affaibliraient la sécurité numérique. Il relève que des entreprises craignent que l'obligation de procéder à des scannages entre en conflit avec d'autres juridictions, rendant la conformité complexe et freinant l'innovation. L'orateur estime que cette problématique est pertinente pour *money control*, car une tension similaire existe dans le secteur financier et fiscal. Selon lui, la Belgique veut renforcer son autonomie fiscale en centralisant le *data mining*, mais risque en même temps des conflits avec les règles européennes relatives à la protection

het risico in conflict te komen met de Europese regels inzake gegevensbescherming, transparantie en evenredigheid. Net zoals *chat control* de grondslagen van de rechtsstaat onder druk zet, onder meer de bescherming van de persoonlijke levenssfeer, valt niet uit te sluiten dat *money control* al dan niet gewild de rechtsonzekerheid voor de burgers vergroot, met ernstige gevolgen.

De spreker gaat vervolgens in op de technische grondslagen van *chat control* en de relevantie ervan voor *money control*. Hij licht toe dat *hash matching* het klassieke instrument is van die architectuur: digitale beelden worden omgezet in unieke vingerafdrukken (*hashes*) die worden vergeleken met databanken van onwettige elementen. Hoewel die vingerafdrukken gepseudonimiseerd zijn, blijven ze gelinkt aan individuen en kunnen ze worden gekruist met bekende gegevens. Die techniek is robuust voor gegevens die exact overeenkomen, maar is gevoelig voor kleine wijzigingen, waardoor de daders door middel van triviale veranderingen aan detectie kunnen ontsnappen. Nog belangrijker is volgens het lid dat de grootschalige toepassing ervan onvermijdelijk leidt tot valspositieven wanneer de databanken onvolledig, verouderd of slecht gecontroleerd zijn. Volgens de heer Vereeck is het probleem voor het CAP vergelijkbaar: financiële risicoprofielen kunnen alleen betrouwbaar zijn indien de referentiegegevens volledig, actueel en correct gekalibreerd zijn. Daarover staat niets in het voorliggende wetsontwerp. De spreker pleit voor bijkomende wetgeving die de transparantie en actualisering van de gebruikte modellen garandeert. Hij beklemtoont dat de massale uitbreiding van datamining het risico op fouten verhoudingsgewijs vergroot, vooral wanneer de algoritmen gebaseerd zijn op historische gegevens en zelfs als ze artificiële intelligentie integreren. Bij gebrek aan bijkomende wetgeving vallen dergelijke systemen veeleer onder de noemer “probabilistische analyses” dan onder fraudebestrijding.

De heer Vereeck gaat ook in op de “contextuele blindheid” van dataminingstechnieken, die volgens hem een menselijk optreden vereist om ernstige fouten te voorkomen. Voor onbekend materiaal schrijft *chat control* voor dat leveranciers artificiële-intelligentiemodellen gebruiken die patronen kunnen herkennen op basis van omvangrijke trainingsgegevenssets. Volgens het lid zijn die sets echter historisch en zijn de modellen probabilistisch van aard: ze geven classificatiewaarschijnlijkheden aan, geen zekerheden. De spreker wijst erop dat zulks een fundamenteel rechtszekerheidsprobleem met zich brengt: mensen of bedrijven kunnen zonder vaststaand bewijs een doelwit worden op basis van statistische algoritmen. Hij illustreert dat risico aan de hand van getuigenissen van bedrijven die met gecombineerde controles (belasting-, sociale en btw-controle) worden geconfronteerd, waarbij de inspecteurs uitdrukkelijk

des données, à la transparence et à la proportionnalité. Il souligne que, tout comme *chat control* met sous pression les fondements de l'État de droit, notamment la protection de la vie privée, *money control* pourrait, volontairement ou non, accroître l'insécurité juridique pour les citoyens, avec des conséquences sérieuses.

L'orateur aborde ensuite les fondements techniques de *chat control* et leur pertinence pour *money control*. Il explique que le *hash matching* constitue l'instrument classique de cette architecture: les images numériques sont converties en empreintes uniques (les *hashes*) comparées à des bases de données d'éléments illégaux. Bien que pseudonymisées, ces empreintes restent associées à des individus et peuvent être confrontées à des données connues. Cette technique, robuste pour des correspondances exactes, est toutefois sensible aux modifications mineures, permettant aux auteurs d'échapper à la détection par des transformations triviales. Plus important encore, selon le député, son application à grande échelle entraîne inévitablement des faux positifs lorsque les bases de données sont incomplètes, obsolètes ou mal contrôlées. Selon M. Vereeck, le problème est analogue pour le PCC: les profils de risque financiers ne peuvent être fiables que si les données de référence sont complètes, actuelles et correctement calibrées, ce qui n'est pas prévu dans le projet de loi à l'examen. Il plaide pour une législation complémentaire garantissant la transparence et la mise à jour des modèles utilisés. Il souligne que l'extension massive du *data mining* accroît proportionnellement le risque d'erreurs, surtout lorsque les algorithmes reposent sur des données historiques, même lorsqu'ils intègrent l'intelligence artificielle. À défaut, ces systèmes ne relèvent pas de la lutte contre la fraude, mais d'une analyse probabiliste.

M. Vereeck aborde également la “cécité contextuelle” des techniques de *data mining*, qui impose selon lui une intervention humaine pour éviter des erreurs graves. Pour le matériel inconnu, *chat control* prévoit que les fournisseurs utilisent des modèles d'intelligence artificielle capables de reconnaître des schémas à partir de vastes ensembles de données d'entraînement. Or, selon le membre, ces ensembles sont historiques et les modèles sont de nature probabiliste: ils indiquent des probabilités de classification, non des certitudes. L'orateur souligne que cela pose un problème fondamental de sécurité juridique: des personnes ou des entreprises peuvent être ciblées sans preuve certaine, sur la base d'algorithmes statistiques. Il illustre ce risque par des témoignages d'entreprises confrontées à des contrôles combinés (fiscal, social, TVA), où les inspecteurs déclarent explicitement qu'ils ne quitteront pas les lieux

verklaren dat ze het bedrijf niet zullen verlaten zonder een inbreuk te hebben vastgesteld, wegens opgelegde rendementsdoelstellingen.

Volgens de heer Vereeck creëert het gebruik van AI-gegenereerde algoritmen geen zekerheid, maar net een structurele onzekerheid: valspositieven kunnen onschuldige gegevens als verdacht aanmerken, terwijl valsnegatieven reële gevallen van misbruik door de mazen van het net laten glijpen. Het lid wijst erop dat die fouten zowel in de wetenschap als in het recht welbekend zijn: hoeveel onschuldigen worden onterecht veroordeeld en hoeveel schuldigen ontsnappen aan vervolging? In een rechtsstaat geldt de eerste fout als ernstiger dan de tweede. Voor hem komt de grootschalige toepassing van deze modellen in fiscale aangelegenheden neer op de aanvaarding van een systeem waarin willekeur en waarschijnlijkheid de plaats innemen van rechtszekerheid.

De spreker wijst op een structureel risico: de meeste van die modellen zijn niet in staat de context te interpreteren. Die contextuele blindheid is bijzonder gevaarlijk in het raam van grootschalig toezicht. Wat de financiële datamining via het CAP betreft, is de heer Vereeck van oordeel dat die leidt tot misleidende correlaties tussen bepaalde transacties of rekeningen, die worden geïnterpreteerd als risico-indicatoren zonder acht te slaan op de omstandigheden. Hij noemt het voorbeeld van een grote financiële familiale overdracht of seizoensgebonden transacties, die mogelijk ten onrechte als verdacht worden aangemerkt. Volgens hem is de parallel met *chat control* duidelijk: probabilistische systemen worden voorgesteld als systemen die deterministische zekerheid bieden, wat de burgers en de media om de tuin leidt.

De heer Vereeck vestigt ook de aandacht op een bijkomend risico, namelijk dat het model in omgekeerde zin wordt gebruikt. Het gaat daarbij om aanvallen waardoor mensen met kwade bedoelingen elementen van de trainingsdata via een manipulatie van het model kunnen reconstrueren. Dat risico is bijzonder zorgwekkend indien de modellen door gevoelige data worden gevoed, zoals beelden van kindermisbruik maar ook fiscale gegevens. Volgens hem is er nog steeds geen afdoend antwoord op de vraag in hoeverre het CAP voldoende is beveiligd: alle waarborgen ten spijt is geen enkel systeem onkwetsbaar; getuige daarvan de talrijke recente hackings van overheidswebsites. De heer Vereeck benadrukt de ernst van de gevolgen, mocht het CAP gehackt worden: gegevens kunnen worden verwijderd of gemanipuleerd, er kunnen vergissingen optreden bij de selectie van dossiers en de fiscale controles zouden minder betrouwbaar worden. Nog onrustwekkender volgens hem is dat men totaal in het ongewisse zou kunnen blijven over het feit dat de dataminingmodellen of hun trainingsprocessen gehackt zijn. Die modellen zijn zo

sans avoir trouvé une infraction, en raison d'objectifs de rendement imposés.

Selon M. Vereeck, l'usage d'algorithmes générés par IA ne crée pas de certitude, mais une incertitude structurelle: des faux positifs peuvent marquer des données innocentes comme suspectes, tandis que des faux négatifs laissent passer des abus réels. Le député rappelle que ces erreurs sont connues en science et en droit: combien d'innocents sont condamnés par erreur et combien de coupables échappent aux poursuites? Dans un État de droit, la première erreur est jugée plus grave que la seconde. Pour lui, appliquer ces modèles à grande échelle dans le domaine fiscal revient à accepter un système où l'arbitraire et la probabilité remplacent la certitude juridique.

L'orateur insiste sur un risque structurel: la plupart de ces modèles sont incapables d'interpréter le contexte. Cette "cécité contextuelle" est particulièrement dangereuse dans un cadre de surveillance massive. En matière de *data mining* financier via le PCC, M. Vereeck estime qu'elle se traduit par des corrélations trompeuses entre certaines transactions ou comptes, interprétées comme des indicateurs de risque sans prise en compte des circonstances. Il cite l'exemple d'un transfert financier familial important ou de transactions saisonnières, susceptibles d'être faussement signalés. Selon lui, le parallèle avec *chat control* est évident: des systèmes probabilistes sont présentés comme offrant une certitude déterministe, ce qui est trompeur pour les citoyens et les médias.

M. Vereeck attire également l'attention sur un risque supplémentaire: celui de l'inversion de modèle. Il explique qu'il s'agit d'attaques permettant à des acteurs malveillants de reconstruire des éléments des données d'entraînement en manipulant le modèle. Ce risque est particulièrement préoccupant lorsque les modèles sont alimentés par des données sensibles, comme des images d'abus d'enfants, mais il vaut également pour les données fiscales. Selon le membre, la question de la sécurité du PCC reste entière: malgré les assurances, il estime qu'aucun système n'est invulnérable, rappelant les nombreux piratages récents de sites de services publics. Le député souligne que si le PCC venait à être compromis, les conséquences seraient graves: suppression ou altération de données, erreurs dans la sélection des dossiers, et perte de fiabilité des contrôles fiscaux. Plus inquiétant encore, selon lui, le piratage des modèles de *data mining* ou de leurs processus d'entraînement pourrait passer totalement inaperçu. Les modèles étant complexes et confidentiels, l'administration fiscale ne pourrait pas détecter une manipulation. L'orateur

complex en vertrouwelijk dat de belastingadministratie weleens niet zou kunnen doorhebben dat ze werden gemanipuleerd. De spreker hekelt de ondoorzichtigheid van die systemen, waarvan de selectiecriteria om strategische redenen geheim worden gehouden. Dat maakt het vrijwel onmogelijk inbreuken op te sporen. De heer Vereeck benadrukt dat miljoenen burgers als gevolg van die kwetsbaarheid kunnen worden getroffen zonder dat er alarmsignalen afgaan.

Tot slot vermeldt hij nog dat de centralisatie van gegevens het risico inhoudt dat nieuwe aanvallen in de hand worden gewerkt. Volgens hem zou een lek bij het CAP of bij de FOD Financiën niet alleen tot een massaal verlies van gegevens, maar ook tot foutieve analyses op grote schaal kunnen leiden. Hij waarschuwt voor het risico op een mogelijke heridentificatie, waarbij individuen alsnog zouden kunnen worden geïdentificeerd door initieel geanonimiseerde gegevensverzamelingen met andere externe databases te vergelijken. Volgens hem waarborgt pseudonimisering geen afdoende anonimiteit, al helemaal niet bij datalekken. De heer Vereeck wijst erop dat met het centraliseren van de financiële gegevens in het CAP een gevoelig doelwit wordt gecreëerd: bij hacking of slechte beveiliging kunnen die gegevens worden geëxploiteerd of verduisterd. Nog volgens hem vertonen de dataminingmodellen van de FOD Financiën structurele kwetsbaarheden. De risico's als gevolg van hacking of van de manipulatie van de modellen kunnen misschien sciencefiction lijken, maar zijn wel degelijk reëel en kunnen ernstige gevolgen hebben. Zo zouden belastingdossiers willekeurig kunnen worden geselecteerd, zonder dat de belastingambtenaren weten waarom die dossiers hun worden toegewezen.

De heer Vincent Van Quickenborne (Open Vld) benadrukt dat het gaat om de bankrekeningen van alle Belgen, ook die van minderjarigen, zij het met een volmacht. Het gaat dus om een aanzienlijke hoeveelheid gegevens. Bovendien kan behalve het CAP ook het datawarehouse te maken krijgen met intrusies. Hoe moeten de gegevens van het ene systeem naar het andere worden overgedragen? De heer Van Quickenborne betreurt dat de deskundigen van het CAP daarover niet eerder werden gehoord. Hij voegt eraan toe dat als tot 20 januari 2026 wordt gedebatteerd, er dan misschien geen regering meer is. Als de regering valt, valt er niets meer te verdedigen.

De heer Lode Vereeck (VB) wijst op een ander probleem: elk model heeft een statistische foutmarge. De spreker haalt het voorbeeld aan van de marge van 0,01 % in het kader van *chat control*. Die marge kan al leiden tot honderdduizenden foutieve meldingen, wat een aanzienlijke foutlast veroorzaakt en zware druk zet op politie, Justitie en andere instanties. Het lid vreest

dénonce le caractère opaque de ces systèmes, dont les critères de sélection sont tenus secrets pour des raisons stratégiques, ce qui rend la détection d'une compromission pratiquement impossible. Il souligne que cette vulnérabilité pourrait affecter des millions de citoyens sans qu'aucune alerte ne soit donnée.

L'orateur évoque enfin le risque lié à la centralisation des données, qui crée un potentiel accru pour de nouvelles attaques. Selon lui, une faille dans le PCC ou au sein du SPF Finances pourrait non seulement entraîner une perte massive de données, mais aussi des analyses erronées à grande échelle. Il met en garde contre la possibilité de réidentification: des ensembles de données, initialement anonymisés, pourraient être recoupés avec d'autres bases externes, permettant d'identifier des individus. Selon le membre, la pseudonymisation ne garantit pas une anonymité durable, surtout en cas de fuite. M. Vereeck souligne que la centralisation des données financières dans le PCC constitue une cible sensible: en cas de piratage ou de mauvaise sécurisation, ces informations pourraient être exploitées ou détournées. De même, selon lui, les modèles de *data mining* utilisés par le SPF Finances présentent des vulnérabilités structurelles. L'orateur rappelle que, bien que cela puisse sembler relever de la science-fiction, les risques liés au piratage des modèles ou à leur manipulation sont bien réels et pourraient avoir des conséquences graves: sélection arbitraire de dossiers fiscaux, sans que les agents sachent pourquoi ces dossiers leur sont attribués.

M. Vincent Van Quickenborne (Open Vld) intervient pour souligner qu'il est question des comptes bancaires de tous les Belges, y compris de ceux des mineurs, certes avec un mandataire, ce qui représente un volume considérable de données. L'orateur indique en outre qu'au-delà du PCC, le *data warehouse* peut également être exposé à des intrusions. Il s'interroge: comment les données doivent-elles être transférées d'un système à l'autre? M. Van Quickenborne déplore qu'une audition des experts du PCC n'ait pas eu lieu plus tôt à ce sujet et ajoute que si les débats se poursuivent jusqu'au 20 janvier 2026, il se peut qu'il n'y ait plus de gouvernement; et si le gouvernement tombe, il n'y aura plus rien à défendre.

M. Lode Vereeck (VB) soulève un autre problème: tout modèle comporte une marge d'erreur statistique. L'orateur cite l'exemple d'une marge de 0,01 % dans le cadre de *chat control*, qui peut déjà entraîner des centaines de milliers de signalements erronés, créant ainsi une charge d'erreurs considérable et exerçant une pression importante sur la police, la Justice et autres.

een soortgelijk effect met *money control* en betreurt het gebrek aan transparantie over de statistische foutmarge, de beveiliging van die databases en de dataminingmodellen. Is er al een test uitgevoerd met dat dataminingmodel? Werden er fouten vastgesteld? De heer Vereeck meent dat een foutenlast, ongeacht de oorzaak en of het nu gaat om een gewone statistische fout, onjuiste gegevens of een onjuiste analyse, een enorme druk zet op Justitie en de FOD Financiën, die nu al kampen met personeelstekort.

De heer Vincent Van Quickenborne (Open Vld) kaart de situatie bij de FOD Financiën aan. Hij wijst erop dat de FOD Financiën in 1999 38.000 medewerkers telde. Dat aantal is sindsdien sterk gedaald, wat aantoonde dat er binnen de administratie besparingen mogelijk zijn. De spreker verduidelijkt ook dat die evolutie verband houdt met de invoering van intelligentere processen waardoor de efficiëntie is verbeterd.

De heer Lode Vereeck (VB) laat weten dat hij beschikt over cijfers van vijf tot zes jaar geleden. Het aantal ambtenaren bij de FOD Financiën werd toen op 28.000 geraamd. Hij stelt vast dat dit aantal geleidelijk is gedaald, tot 24.000 volgens de laatst bekende cijfers. Thans zijn het er waarschijnlijk minder dan 20.000. De spreker benadrukt dat België niettemin relatief veel belastingambtenaren per inwoner telt en is van oordeel dat zou moeten worden onderzocht of er ondanks de sterke personeelsvermindering nog efficiëntiewinsten mogelijk zijn. Voorts stelt de spreker vast dat naarmate het aantal inspecteurs afnam, meer indienstnemeningen hebben plaatsgevonden in de ondersteunende diensten, met name op het gebied van personeel en organisatie (P&O). Dat wijst op het toenemende belang van die functies.

Vervolgens vestigt de spreker de aandacht op een soortgelijk probleem met betrekking tot de fiscaliteit en het gebruik van datamining. Wanneer risicoanalyses worden toegepast op miljoenen rekeningen, kunnen statistische foutmarges en gebrekkige gegevens zich opstapelen en zich uitbreiden. Hij waarschuwt voor het overmatig controleren van onschuldige burgers, terwijl de echte fraudeurs aan opsporing ontsnappen. Hij is van oordeel dat het breed inzetten van datamining niet noodzakelijk doeltreffendere resultaten oplevert, maar mogelijk zelfs contraproductief is. Hij brengt in herinnering dat datamining vroeger al werd gebruikt, maar dan voor individuele gevallen. Die gerichte aanpak verschilt fundamenteel van een massale toepassing op de gehele bevolking, zoals het thans ter bespreking voorliggende wetsontwerp beoogt.

De spreker gaat in op de zogenaamde *function creep*. Bij technologische toepassingen zoals opsporing via

Le député craint un effet similaire avec *money control* et déplore le manque de transparence concernant la marge d'erreur statistique, la sécurisation de ces bases de données et les modèles de *data mining*. Il s'interroge: un test a-t-il déjà été réalisé avec ce *data mining*? Des erreurs ont-elles été détectées? M. Vereeck estime qu'une charge d'erreurs, quelle qu'en soit la cause, qu'il s'agisse d'une simple erreur statistique, d'une donnée défectueuse ou d'une analyse incorrecte, exerce une pression énorme sur la Justice et sur le SPF Finances, qui manquent de personnel.

M. Vincent Van Quickenborne (Open Vld) intervient pour évoquer la situation au SPF Finances. Il indique qu'en 1999, le SPF Finances comptait 38.000 agents. Ce chiffre a fortement diminué depuis, ce qui démontre qu'il est possible de réaliser des économies au sein de l'administration. L'orateur précise également que cette évolution est liée à la mise en place de processus plus intelligents qui ont permis d'améliorer l'efficacité.

M. Lode Vereeck (VB) indique qu'il disposait de chiffres datant de cinq à six ans, estimant alors à 28.000 le nombre d'agents au SPF Finances et constate que ce nombre a progressivement diminué, passant à 24.000 selon les derniers chiffres connus, et probablement à moins de 20.000 aujourd'hui. L'orateur souligne que la Belgique compte néanmoins relativement beaucoup d'agents fiscaux par habitant et estime qu'il faudrait examiner si des gains d'efficacité restent possibles, malgré la forte réduction des effectifs. Par ailleurs, le député observe que les recrutements dans les services d'appui, notamment en matière de personnel et d'organisation (P&O), ont augmenté à mesure que le nombre d'agents diminuait, ce qui témoigne de l'importance croissante de ces fonctions.

L'orateur attire ensuite l'attention sur une problématique similaire concernant la fiscalité et le recours au *data mining*. Lorsque des analyses de risque sont appliquées à des millions de comptes, les marges d'erreur statistique et les données défectueuses peuvent se cumuler et s'amplifier. Il met en garde contre le risque de "surcontrôle" de citoyens innocents, alors que les véritables fraudeurs échappent à la détection. Selon lui, l'ampleur du déploiement du *data mining* ne le rend pas nécessairement plus efficace, mais potentiellement contre-productif. Il rappelle qu'auparavant, le *data mining* était déjà utilisé, mais de manière individualisée. Cette approche ciblée diffère fondamentalement d'une application massive à l'ensemble de la population, telle que prévue dans le projet de loi à l'examen.

L'orateur souhaite également aborder la *function creep*. Dans le cadre de technologies telles que la détection

kunstmatige intelligentie en datamining is *function creep* een bekend verschijnsel: een tool die voor een specifiek en welomlijnd doel werd ontworpen, wordt uiteindelijk uitgebreid toegepast in het raam van nieuwe contexten. Dergelijke ontsporingen kunnen zich technisch gezien almaar makkelijker voordoen daar de architectuur al bestaat en ze alleen opnieuw hoeft te worden geconfigureerd. Volgens de heer Vereeck bestaat dat risico voor *chat control* maar evenzeer voor *money control*, wat zou betekenen dat detectiemodules snel zouden kunnen worden aangepast om ook andere misdrijven op te sporen, gedragsanalyses te maken of zelfs sociale risicoprofielen te bepalen, soms zonder parlementair toezicht.

De spreker licht toe dat de *function creep* op fiscaal en financieel gebied een risico is dat thans nadrukkelijk in België bestaat. Een systeem zoals het CAP, dat oorspronkelijk werd ontworpen om ernstige georganiseerde fraude op te sporen, zou kunnen worden uitgebreid met het oog op de opsporing van fiscale optimalisatie of sociale fraude, of voor vermogenstoezicht. De spreker erkent dat het wetsontwerp nog voorziet in een menselijke tussenkomst na de selectie, maar hij acht zulks onvoldoende: de ambtenaar moet niet alleen de controle uitvoeren, maar ook kunnen uitleggen waarom het dossier aan hem werd toegewezen, wat thans niet het geval is.

De heer Vereeck waarschuwt dat de volgende logische stap dan de volledig automatische fiscale controle zal zijn, zonder menselijke tussenkomst. Hij stelt dat als de regering thans zonder scrupules om politieke redenen in die zin handelt, het vrijwel zeker is dat een volledige automatisering zal volgen.

De heer Lode Vereeck (VB) kondigt aan de *function creep* uitvoeriger te zullen behandelen in zijn diepgaandere analyse van “*money control*”.

Hij stelt dat de juridische grondslagen van “*chat control*” bijna één op één overgezet kunnen worden naar “*money control*”, met vergelijkbare bezorgdheden rond privacy, gegevensbescherming en vrijheid van meningsuiting.

Het Handvest van de Grondrechten van de Europese Unie is het primaire juridische kader waarbinnen “*chat control*” moest worden beoordeeld. Centraal zijn artikelen 7 (recht op eerbiediging van het privéleven en familie- en gezinsleven – privacy), 8 (recht op bescherming van persoonsgegevens) en 11 (vrijheid van meningsuiting en informatie).

Artikel 7 omvat ook de vertrouwelijkheid van de communicatie. De spreker wijst erop dat “*chat control*” een

par intelligence artificielle et le *data mining*, le *function creep* est un phénomène bien connu: un outil conçu pour un objectif spécifique et limité finit par être étendu à de nouveaux contextes d'utilisation. Cette dérive est d'autant plus facile sur le plan technique que l'architecture existe déjà et qu'il suffit de la reconfigurer. Selon M. Vereeck, c'est le cas pour *chat control*, mais aussi pour *money control*, ce qui permet d'étendre rapidement les modules de détection à d'autres infractions, à des analyses comportementales ou même à des profils de risque social, parfois sans contrôle parlementaire.

L'intervenant explique que, dans le domaine fiscal et financier, le *function creep* constitue aujourd'hui en Belgique un risque aigu. Un système tel que le PCC, conçu à l'origine pour détecter la fraude organisée grave, pourrait être élargi à la fiscalité optimisée, à la fraude sociale ou à la surveillance des patrimoines. L'orateur reconnaît que le projet actuel prévoit encore une intervention humaine après la sélection, mais estime que cela ne suffit pas: le fonctionnaire doit non seulement effectuer le contrôle, mais aussi pouvoir expliquer pourquoi le dossier lui a été attribué, ce qui n'est pas le cas.

M. Vereeck avertit que la prochaine étape logique sera la complète automatisation du contrôle fiscal, sans intervention humaine. Il affirme en effet que si le gouvernement agit ainsi aujourd'hui, sans scrupules, pour des raisons politiques, il est presque certain que la dérive vers une automatisation totale suivra.

M. Lode Vereeck (VB) annonce qu'il examinera plus en détail la question du détournement de finalité (*function creep*) dans le cadre de son analyse approfondie de *money control*.

Il indique que les fondements juridiques de *chat control* peuvent être transposés presque tels quels à *money control*, les préoccupations étant similaires en ce qui concerne le respect de la vie privée, la protection des données et la liberté d'expression.

La Charte des droits fondamentaux de l'Union européenne est le cadre juridique principal qui devait servir de prisme pour l'évaluation de *chat control*. Les articles 7 (droit au respect de la vie privée et familiale), 8 (droit à la protection des données à caractère personnel) et 11 (liberté d'expression et d'information) sont essentiels à cet égard.

L'article 7 vise également la confidentialité des communications. L'intervenant souligne que *chat control*

structurele inbreuk vormt op deze vertrouwelijkheid van communicatie door het scannen zonder concrete aanwijzing van misdrijf, en dat deze logica ook geldt voor “*money control*”.

Volgens de rechtspraak van het Hof van Justitie van de Europese Unie zijn ongerichte en massale ingrepen slechts onder uitzonderlijke omstandigheden toegestaan en moeten deze voldoen aan noodzakelijkheid, proportionaliteit en doelbinding. Ook in het kader van “*money control*” gelden dezelfde grondrechten.

Het CAP-systeem verwerkt gegevens die rechtstreeks verband houden met het privéleven en de financiële autonomie van burgers. De spreker stelt dat de reflectie uit het EU-Handvest, waarin algemene en niet-gerichte monitoring als problematisch wordt beschouwd, evenzeer geldt voor de massale datamining binnen “*money control*”. Indien het scannen van communicatie volgens Europese normen te ver gaat, dan geldt dit ook voor ongerichte screening van financiële gegevens.

Het lid heeft het dan over het Europees Verdrag voor de Rechten van de Mens (EVRM) dat een aanvullende bescherming biedt. Zo waarborgt artikel 8 van het EVRM het recht op bescherming van privéleven en communicatie.

Het Europees Hof voor de Rechten van de Mens heeft herhaaldelijk geoordeeld dat algemene *surveillance* zonder concrete verdenking in strijd is met artikel 8 van het EVRM. Daar zijn een reeks arresten over geveld die bevestigen dat staten verplicht zijn om krachtige juridische waarborgen te voorzien bij elke vorm van interceptie of monitoring. “*chat control*”, dat scanning toelaat zonder rechterlijk bevel en zonder individuele verdenking, voldoet niet aan deze voorwaarden.

De spreker verwijst naar het SyRI-arrest in Nederland, waarbij een systeem van grootschalige, ondoorzichtige en geheime datamining met geheime protocollen door de rechter werd vernietigd wegens disproportionaliteit en gebrek aan transparantie voor burgers.

Hij benadrukt dat dezelfde juridische logica toepasselijk is op “*money control*”, waardoor de proportionaliteit van dit systeem rechtstreeks ter discussie staat. Indien “*chat control*” juridisch onhoudbaar is wegens massale screening, dan bevindt datamining zich in een gelijkaardige risicozone.

constitue une atteinte structurelle à cette confidentialité des communications dès lors qu’il prévoit de scanner toutes les communications sans qu’il existe la moindre indication concrète d’infraction, et que cette logique s’appliquera également à *money control*.

Selon la jurisprudence de la Cour de justice de l’Union européenne, les interventions non ciblées et de masse ne sont autorisées que dans des circonstances exceptionnelles et doivent respecter les principes de nécessité, de proportionnalité et de limitation de la finalité. Ces principes fondamentaux s’appliquent également à *money control*.

Le système PCC traite des données directement liées à la vie privée et à l’autonomie financière des citoyens. L’intervenant indique que le principe contenu dans la Charte de l’Union européenne, qui considère qu’un contrôle généralisé et non ciblé est problématique, s’applique également à l’exploration massive de données dans le cadre de *money control*. Si le scannage des communications va trop loin au sens des normes européennes, cela vaut aussi pour le scannage non ciblé des données financières.

L’intervenant évoque ensuite la Convention européenne des droits de l’homme (ConvEDH) qui offre une protection supplémentaire. Par exemple, l’article 8 de la ConvEDH garantit le droit au respect de la vie privée et de la correspondance.

La Cour européenne des droits de l’homme a estimé à plusieurs reprises que la *surveillance* généralisée qui ne repose pas sur des soupçons concrets est contraire à l’article 8 de la ConvEDH. Plusieurs arrêts ont été rendus en ce sens, confirmant que les États sont tenus de prévoir des garanties juridiques solides pour toute forme d’interception ou de contrôle. *chat control* qui autoriserait le scannage en l’absence de toute injonction judiciaire et de toute suspicion individuelle, ne remplit pas ces conditions.

L’intervenant renvoie à l’arrêt SyRI rendu aux Pays-Bas, par lequel le juge a mis fin à un système d’exploration des données à grande échelle, opaque et secret, assorti de protocoles secrets, en raison de son caractère disproportionné et de son manque de transparence à l’égard des citoyens.

Il souligne que la même logique juridique s’applique à *money control*, ce qui remet directement en question la proportionnalité de ce système. Si *chat control* est juridiquement indéfendable en raison du scannage de masse, l’exploration des données présente toutefois aussi des risques similaires.

Het SyRI-arrest biedt, volgens het Kamerlid, een houvast indien de huidige *function creep* van het CAP-systeem zich verder ontwikkelt, aangezien ook dit systeem mogelijk de wettelijke toetsing niet zal doorstaan.

Daarna behandelt de heer Vereeck de Algemene Verordening Gegevensbescherming (AVG), die ook strikte voorwaarden stelt aan gegevensverwerking. Hij stelt vast dat “*chat control*” op meerdere punten hiermee in strijd lijkt te zijn.

Zo ondermijnt de voorgestelde scanning het principe van dataminimalisatie, aangezien alle communicatie wordt gescand, en is ook de doelbinding problematisch, net zoals bij “*money control*”.

Ten derde vereist de richtlijn transparantie in besluitvorming en verwerking. “*chat control*” voorziet echter niet dat burgers inzicht krijgen in de algoritmische processen die hun communicatie beoordelen. Dat is, voorlopig althans, ook niet de bedoeling voor “*money control*”.

Verder benadrukt de spreker dat menselijke tussenkomst, zoals vereist door artikel 22 van de AVG, onvoldoende is gewaarborgd. Bij “*chat control*” vindt screening grotendeels automatisch plaats, met menselijke beoordeling pas in een latere fase, wat indruist tegen de richtlijn.

De spreker ziet bij CAP-datamining dezelfde spanningen: gebrek aan transparantie, geen inzicht voor burgers in selectiecriteria en een potentieel gebruik van data voor bredere doelstellingen.

Hij besluit dat de juridische analyses die “*chat control 1.0*” onderuit halen, met geringe aanpassingen ook toepasbaar zijn op “*money control*”, wat de kwetsbaarheid van het fiscale dataminingmodel onderstreept.

Veel lidstaten beschikken ook over sterke grondwettelijke waarborgen omtrent privacy, communicatiegeheim en rechtsbescherming. Nationale hoven hebben in het verleden al maatregelen ongeldig verklaard die te ver gingen in digitale *surveillance*. Het is waarschijnlijk dat “*chat control*” indien ingevoerd, ook in de versie 2.0, constitutioneel zal worden aangevochten.

Nationale grondwetten, zoals in Duitsland en Nederland, vereisen immers een strikte proportionaliteitstoetsing en verbieden verregaande monitoring zonder individuele aanleiding. Ook de Belgische Grondwet biedt

Selon l'intervenant, l'arrêt SyRI pourrait servir de repère si le système du PCC continue à être détourné de sa finalité, car ce système pourrait également ne pas résister au contrôle de légalité.

M. Vereeck évoque ensuite le Règlement général sur la protection des données (RGPD), qui impose également des conditions strictes en matière de traitement des données. Il constate que plusieurs éléments de *chat control* semble contraire à ce règlement.

Par exemple, le scannage proposé porterait atteinte au principe de minimisation des données, puisque toutes les communications seraient scannées, et la limitation de la finalité poserait également problème, comme pour *money control*.

Troisièmement, la directive exige la transparence dans la prise de décision et le traitement. Or, *chat control* ne prévoit pas de permettre aux citoyens d'accéder aux processus algorithmiques qui analysent leurs communications. *Money control* ne le prévoit pas non plus, du moins pour l'instant.

L'intervenant souligne en outre que l'intervention humaine, telle que requise par l'article 22 du RGPD, n'est pas suffisamment garantie. *chat control* prévoit un scannage principalement automatique, l'évaluation humaine n'intervenant qu'à un stade ultérieur, ce qui est contraire à la directive.

L'intervenant constate que les mêmes problèmes se posent en cas de recours à l'exploration des données dans le PCC: manque de transparence, absence d'information des citoyens sur les critères de sélection et utilisation potentielle des données à des fins plus larges.

Il conclut en indiquant que les analyses juridiques qui invalident *chat control 1.0* s'appliquent également, moyennant quelques modifications mineures, à *money control*, ce qui met en lumière la vulnérabilité du modèle d'exploration des données fiscales.

De nombreux États membres disposent également de garanties constitutionnelles solides en matière de respect de la vie privée, de secret des communications et de protection juridique. Par le passé, des cours nationales ont déjà annulé des mesures qui allaient trop loin en matière de *surveillance* numérique. Il est probable que, même dans sa version 2.0, *chat control*, s'il est instauré, soit attaqué sur le plan constitutionnel.

Des Constitutions nationales, comme les Constitutions allemande et néerlandaise, exigent en effet un contrôle strict de la proportionnalité et interdisent toute surveillance excessive en l'absence de motif individuel. La

bescherming van privéleven, van correspondentie en van eigendom. De spreker concludeert dat systemen als “*chat control*” en “*money control*”, die niet-gerichte datamining mogelijk maken zonder transparantie en proportionaliteit, grote juridische risico's lopen.

De spreker kondigt dan aan later nog uitgebreid te willen ingaan op “*chat control*” en bij uitbreiding “*money control*”. Hij wil daarbij de ethische grondslagen bespreken, zoals ongericht toezicht, menselijke waardigheid, controle over persoonlijke gegevens, discriminatie en algoritmische bias, evenals het verlies van vertrouwen en de ethiek van relaties. Daarnaast wil hij de maatschappelijke gevolgen behandelen, waaronder vertrouwen en legitimiteit van de overheid, de opkomst van een nieuwe digitale cultuur, economische gevolgen, de verhouding tussen burger en digitale infrastructuur en risico's voor sociale cohesie. Hij zal ook andere kritische perspectieven en mogelijke alternatieven voorleggen.

De heer Vincent Van Quickenborne (Open Vld) kondigt aan dat hij een vergelijking zal maken tussen het Belgische CAP-systeem en het Zweedse model.

Hij wijst op belangrijke verschillen: in Zweden is het CAP privaat en gedecentraliseerd, terwijl het in België bij de Nationale Bank zit onder toezicht van de thesaurie.

Zweden kent geen wettelijke basis voor profilering, terwijl België die expliciet invoert.

Toegang tot gegevens gebeurt in Zweden enkel op gemotiveerd verzoek, bij ons permanent en automatisch.

Zweden voorziet kennisgeving aan burgers, België niet. Het lid vraagt de minister of hij een kennisgevingsplicht voorziet. Hij merkt verder op dat burgers in België slechts vier tot vijf keer per jaar een logboek opvragen, terwijl het CAP jaarlijks meer dan 300.000 keer door informatiegerechtigden wordt geraadpleegd.

Het toezicht ligt in Zweden bij het parlement, in België bij de GBA met beperkte bevoegdheid.

Met andere woorden, er is in Zweden een functionele scheiding tussen beheer, gebruik en toezicht, in België niet.

Constitution belge garantit également la protection de la vie privée, de la correspondance et de la propriété. L'intervenant conclut en indiquant que des systèmes tels que *chat control* et *money control*, qui permettent une exploration des données non ciblée en l'absence de toute transparence et de toute proportionnalité, prêtent le flanc à des risques juridiques importants.

L'intervenant annonce son intention d'évoquer ensuite plus en détail *chat control* et, par extension, *money control*. Il souhaite à cet égard s'intéresser à leurs fondements éthiques, par exemple la surveillance non ciblée, la dignité humaine, le contrôle des données à caractère personnel, la discrimination et les biais algorithmiques, ainsi que la perte de confiance et l'éthique des relations. Il souhaite également évoquer les conséquences sociales, notamment la confiance dans les pouvoirs publics et la légitimité de ceux-ci, l'émergence d'une nouvelle culture numérique, les conséquences économiques, la relation entre les citoyens et les infrastructures numériques et les risques pour la cohésion sociale. Il présentera également d'autres perspectives critiques et d'éventuelles solutions alternatives.

M. Vincent Van Quickenborne (Open Vld) annonce qu'il va effectuer une comparaison entre le système belge du PCC et le modèle suédois.

Il relève des différences de taille. En Suède, le PCC est privé et décentralisé alors qu'en Belgique, il relève de la Banque nationale et est sous la supervision de la Trésorerie.

La Suède n'a pas de base légale permettant le profilage alors que la Belgique en instaure explicitement un.

En Suède, l'accès aux données se fait uniquement sur demande motivée; chez nous, cet accès est permanent et automatique.

La Suède avertit les citoyens lorsqu'ils font l'objet d'un contrôle; la Belgique, pas. Le membre demande au ministre s'il prévoit d'instituer une obligation de notification. Il fait ensuite observer que les citoyens belges ne réclament un journal des opérations que quatre à cinq fois par an, alors que le PCC est consulté plus de 300.000 fois par les personnes habilitées à recevoir l'information.

En Suède, le contrôle est confié au parlement. En Belgique, il est confié à l'APD, qui dispose de compétences limitées.

En d'autres termes, la Suède applique une séparation fonctionnelle entre la gestion, l'utilisation et le contrôle. En Belgique, ce n'est pas le cas.

De spreker besluit dat Zweden een cultuur van transparantie en “*open government, closed data*” kent, terwijl België evolueert naar “*closed government, open data*”, wat hij als een brug te ver bestempelt.

Het Kamerlid gaat daarna in op de grondrechtelijke proportionaliteit en wijst erop dat Zweden een drievoudige verankering kent: in de privacywet (*Personuppgiftslagen* (1998:204), artikel 2.6), in de wet ter uitvoering van de AVG (*Dataskyddslag* (2018:218)) en in de rechtspraak van het Hooggerechtshof voor administratieve geschillen (*Högsta förvaltningsdomstolen* (HFD)).

Elke inmenging moet wettelijk voorzien zijn, evenredig met het doel en een legitiem doel dienen. De spreker stelt dat het Belgische systeem van “*money control*” deze toets niet doorstaat: er is geen individuele noodzakelijkheid, de inmenging is algemeen en disproportioneel.

De heer Van Quickenborne benadrukt dat Zweden efficiëntie combineert met minimale inmenging: een inningsgraad van 99,1 %, minder intrusieve bevoegdheden en 40 % lagere toezichtskosten per geïnde euro. Dit succes berust op informatiediscipline, transparantie en rechtsbescherming, terwijl België kampt met verouderde wetgeving, onduidelijke instructies en controles die vaak stranden bij de rechtbank, wat de efficiëntie ondermijnt.

Het lid formuleert vervolgens vijf aanbevelingen.

Ten eerste vraagt hij om een kennisgevingsplicht, zodat burgers automatisch geïnformeerd worden bij consultatie van het CAP.

Ten tweede pleit hij voor beperking van gegevensverwerking tot concrete gevallen van zware fraude, met respect voor proportionaliteit en transparantie.

Ten derde vraagt hij om een functionele scheiding tussen beheer, gebruik en toezicht.

Ten vierde wil hij een verbod op profilering en datamining zonder duidelijke en transparante wettelijke basis.

Ten vijfde dringt hij aan op meer transparantie en publieke controle, inclusief een jaarlijks verslag aan het Parlement zoals wettelijk voorzien.

De spreker gaat dan over tot een vergelijking tussen het Belgische CAP-systeem en het Finse model.

L'intervenant en conclut que la Suède possède une culture de transparence conforme au principe “*open government, closed data*”, tandis que la Belgique évolue vers une philosophie “*closed government, open data*”, ce qui revient à franchir une ligne rouge à ses yeux.

Le membre aborde ensuite la proportionnalité au regard des droits fondamentaux et indique que la Suède connaît un triple ancrage: la loi relative à la vie privée (*Personuppgiftslagen* (1998:204), article 2.6); la loi portant exécution du RGPD (*Dataskyddslag* (2018:218)) et la jurisprudence de la cour supérieure des contentieux administratifs (*Högsta förvaltningsdomstolen* (HFD)).

Toute ingérence doit s'appuyer sur une base légale, être proportionnelle à l'objectif poursuivi et servir un but légitime. L'intervenant indique que le système de *money control* ne satisfait pas à ces critères: il n'y a pas de nécessité individuelle et l'ingérence est généralisée et disproportionnée.

M. Van Quickenborne souligne que la Suède parvient à marier efficacité et ingérence minimale. Elle obtient un taux de perception de 99,1 %, applique des compétences moins intrusives et débourse 40 % de frais de contrôle en moins par euro perçu. Cette réussite repose sur la discipline dans le traitement des informations, la transparence et la protection juridique. Pendant ce temps-là, la Belgique se heurte à une législation obsolète, à des instructions floues et à des contrôles qui finissent souvent devant les tribunaux, ce qui mine l'efficacité.

Le membre formule ensuite cinq recommandations.

Premièrement, il demande l'introduction d'une obligation de notification pour que les citoyens soient automatiquement informés en cas de consultation du PCC.

Deuxièmement, il plaide pour la limitation du traitement des données aux cas concrets de fraude grave, dans le respect des principes de proportionnalité et de transparence.

Troisièmement, il demande une séparation fonctionnelle entre la gestion, l'utilisation et le contrôle.

Quatrièmement, il réclame une interdiction du profilage et du *data mining* sans base légale claire et transparente.

Cinquièmement, il demande instamment plus de transparence et de contrôle public, notamment par le biais d'un rapport annuel à remettre au Parlement, comme la loi le prévoit.

L'intervenant procède ensuite à une comparaison entre le système du PCC belge et le modèle finlandais.

Finland wordt beschouwd als een van de meest evenwichtige en rechtsstatelijke landen wat betreft het beheer van persoonsgegevens door de overheid. De controle op fiscale en financiële gegevens steunt er op drie pijlers.

Ten eerste is er de legaliteitspijler: elke verwerking van gegevens is uitdrukkelijk bij wet geregeld, met een duidelijke afbakening van doel en bevoegdheid.

Ten tweede geldt een institutionele scheiding: degene die de gegevens beheert, is niet dezelfde als degene die ze gebruikt.

Ten derde zijn vertrouwen en transparantie cruciaal.

De spreker benadrukt dat het Finse model grondig verschilt van het Belgische en van *“money control”*. Finland kiest voor decentralisatie en transparantie en houdt zich strikt aan de AVG. De Finse aanpak wordt omschreven als technologisch vooruitstrevend, maar juridisch ingebed: digitalisering staat er in dienst van de rechtsstaat, niet omgekeerd.

Finland behoort tot de Scandinavische landen met de langste traditie van openbaarheid van bestuur. Het Finse kader is gebaseerd op het principe van *“julkisuusperiaate”*, vastgelegd in de wet van 1951 inzake openbaarheid van overheidsdocumenten. Deze wet verleent elke burger recht op inzage van overheidsinformatie, tenzij de wet uitdrukkelijk een uitzondering bepaalt. Transparantie wordt er beschouwd als een voorwaarde voor verantwoordelijkheid en vormt de basis voor het latere digitale bestuur.

In de fiscale context betekent dit dat burgers weten hoe belastingen worden berekend en dat de overheid geen fiscale databanken mag aanleggen zonder expliciete wettelijke basis.

In 1990 voerde Finland een van de meest geavanceerde digitaliseringsprogramma's van Europa door. De Finse Belastingdienst (*Verohallinto*) ontwikkelde het elektronisch aangiftesysteem Vero.fi en koos daarbij voor dataminimalisatie: enkel gegevens die noodzakelijk zijn voor belastingheffing worden verzameld, steeds binnen een wettelijk kader. Het lid merkt op dat in België naast de digitale aangifte ook nog steeds een papieren aangifte mogelijk is en vraagt naar de verhouding tussen beide indieningswijzen.

De belangrijkste fiscale procedures zijn vastgelegd in wetgeving, zoals de wet op de belastingprocedure

La Finlande est considérée comme l'un des pays les plus équilibrés et les plus respectueux de l'État de droit en ce qui concerne le traitement des données à caractère personnel par les autorités publiques. Le contrôle des données fiscales et financières s'y appuie sur trois piliers.

Tout d'abord, la légalité: chaque traitement de données est régi par la loi, avec une délimitation claire de la finalité et des compétences.

Ensuite, une séparation institutionnelle s'applique: la gestion et l'utilisation des données ne sont pas confiées aux mêmes instances.

Enfin, la confiance et la transparence jouent un rôle capital.

L'intervenant souligne que le modèle finlandais se distingue nettement du modèle belge et du *money control*. La Finlande choisit la décentralisation et la transparence et s'en tient strictement aux règles énoncées par le RGPD. L'approche finlandaise est décrite comme innovante et technologique, mais aussi comme juridiquement ancrée: le numérique est mis au service de l'État de droit et non l'inverse.

La Finlande appartient au monde scandinave, qui dispose de la plus longue tradition en matière de publicité de l'administration. Le cadre finlandais se base sur le principe de *“julkisuusperiaate”*, établi par la loi de 1951 en matière de publicité des documents publics. Cette loi octroie à chaque citoyen un droit de consultation des informations publiques, sauf exception expressément prévue par la loi. La transparence y est vue comme un préalable à la responsabilité et sert de fondement au développement ultérieur de la gouvernance numérique.

Dans le contexte fiscal, ces principes signifient que les citoyens savent comment les impôts sont calculés et que les autorités publiques ne peuvent créer de banques de données fiscales sans base légale expresse.

En 1990, la Finlande a lancé un des programmes de numérisation les plus avancés d'Europe. L'administration fiscale finlandaise (*Verohallinto*) a conçu le système de déclaration électronique Vero.fi, en optant pour la minimisation des données, c'est-à-dire que seules les données nécessaires à la perception des impôts étaient collectées, toujours dans un cadre légal défini. Le membre fait observer qu'en Belgique, outre la déclaration numérique, une version papier est toujours disponible et il demande à connaître le ratio d'utilisation entre les deux méthodes de déclaration.

Les principales procédures fiscales ont été fixées dans la législation, par exemple dans la loi sur la procédure

(*laki verotusmenettelystä*², 1995), en de digitalisering verliep hand in hand met strenge privacywetgeving. De privacywet van 1999 (*henkilötietolaki*³) vormde de basis voor de huidige wet (*tietosuoja*⁴).

In een derde fase, met de Europese anti-witwasrichtlijnen (2015-2018), werd de Finse toezichtsstructuur hervormd.

De wet van 2017 (*Laki rahanpesun ja terrorismin rahoittamisen estämisestä*⁵) verplicht financiële instellingen om ongebruikelijke transacties te melden aan de *Financial Intelligence Unit (FIU)* of *Rahanpesun selvittelykeskus*, de Finse tegenhanger van de CFI.

Daarnaast werd de toezichthouder op financiële markten (*Finanssivalvonta*) versterkt. In België vervult de FSMA een gelijkaardige rol.

Bovendien is Finland sinds 2019 aangesloten bij het internationale *Common Reporting Standard*-netwerk (CRS) voor automatische uitwisseling van financiële gegevens.

De spreker benadrukt dat, ondanks deze internationale gegevensinstroom, het gebruik in Finland nationaal beperkt blijft: gegevens mogen enkel worden gebruikt voor belastingheffing en niet voor profilering of preventieve analyse. Dit contrasteert met de Belgische aanpak, waar ook buitenlandse rekeningen worden opgenomen in een datawarehouse en onderworpen aan "*money control*". Finland hanteert aldus een veel voorzichtiger en privacyvriendelijker beleid.

De spreker gaat vervolgens in op de grondslag van het Finse kader en het ontbreken van een systeem zoals "*money control*".

Hij wijst erop dat dit voortvloeit uit de Finse Grondwet (*Perustuslaki*⁶), waarin artikel 10 een sterke bescherming van de persoonlijke levenssfeer waarborgt. Deze bepaling stelt dat de bescherming van persoonsgegevens voor iedereen gegarandeerd is en dat nadere regels bij wet moeten worden vastgesteld. Dit legaliteitsbeginsel houdt in dat elke inmenging in de privacy of verwerking van persoonsgegevens in een formele wet moet

fiscale (*laki verotusmenettelystä*², 1995), et la numérisation s'est construite dans le respect d'une législation rigoureuse en matière de respect de la vie privée. La loi relative à la protection de la vie privée de 1999 (*henkilötietolaki*³) a constitué la base de la loi actuelle (*tietosuoja*⁴).

Dans une troisième phase, marquée par l'arrivée des directives européennes antiblanchiment (2015-2018), la structure de contrôle finlandaise a été réformée.

La loi de 2017 (*Laki rahanpesun ja terrorismin rahoittamisen estämisestä*⁵) oblige les institutions financières à signaler les transactions inhabituelles à la cellule de renseignement financier (*Financial Intelligence Unit – FIU*) ou au *Rahanpesun selvittelykeskus*, l'équivalent finlandais de la CTIF.

Par ailleurs, l'autorité de surveillance des marchés financiers (*Finanssivalvonta*) a été renforcée. En Belgique, la FSMA joue un rôle similaire.

De plus, depuis 2019, la Finlande est affiliée au réseau international *Common Reporting Standard* (CRS) pour l'échange automatique de données financières.

L'intervenant souligne que, malgré cet afflux de données internationales, l'utilisation des données reste limitée au niveau national en Finlande: elles ne peuvent être utilisées qu'à des fins fiscales et non à des fins de profilage ou d'analyse préventive. Cette approche contraste avec celle de la Belgique, où les comptes étrangers sont intégrés dans une *datawarehouse* et soumis au *money control*. La Finlande adopte ainsi une politique bien plus prudente et bien plus respectueuse de la vie privée.

L'intervenant évoque ensuite les fondements de la législation finlandaise et l'absence d'un système comparable au *money control*.

Il indique que cette situation découle de la Constitution finlandaise (*Perustuslaki*⁶), dont l'article 10 garantit une forte protection de la vie privée. Cette disposition prévoit que la protection des données à caractère personnel est garantie pour chacun et que les modalités doivent être fixées par la loi. Ce principe de légalité implique que toute ingérence dans la vie privée ou tout traitement de données à caractère personnel doit être prévu dans une

² Laki verotusmenettelystä | 1558/1995 | Lainsäädäntö | Finlex.

³ Henkilötietolaki | 523/1999 | Lainsäädäntö | Finlex.

⁴ Tietosuoja | 1050/2018 | Lainsäädäntö | Finlex.

⁵ Laki rahanpesun ja terrorismin rahoittamisen estämisestä | 444/2017 | Lainsäädäntö | Finlex.

⁶ Suomen perustuslaki | 731/1999 | Legislation | Finlex.

² Laki verotusmenettelystä | 1558/1995 | Lainsäädäntö | Finlex.

³ Henkilötietolaki | 523/1999 | Lainsäädäntö | Finlex.

⁴ Tietosuoja | 1050/2018 | Lainsäädäntö | Finlex.

⁵ Laki rahanpesun ja terrorismin rahoittamisen estämisestä | 444/2017 | Lainsäädäntö | Finlex.

⁶ Suomen perustuslaki | 731/1999 | Legislation | Finlex.

zijn opgenomen, met duidelijke doelomschrijving en waarborgen.

Het lid benadrukt dat de Finse rechterlijke macht dit beginsel strikt toepast: een koninklijk besluit, ministerieel besluit of circulaire volstaat niet om aan het legaliteitsbeginsel te voldoen.

Hij verwijst naar het advies van de Raad van State, waarin wordt gesteld dat verwerking van persoonsgegevens enkel op een wettelijke basis kan gebeuren en niet mag worden gedelegeerd. De wet moet bovendien voldoende precies zijn, wat in Finland consequent wordt nageleefd, terwijl dit in België veel minder strikt gebeurt.

Naast de Grondwet is er de wet inzake belastingprocedures (*laki verotusmenettelystä*⁷). Deze wet regelt de bevoegdheden van de Finse Belastingdienst.

Artikel 26 bepaalt dat de *Verhallinto* enkel informatie mag opvragen die noodzakelijk is voor een correcte belastingheffing. De wet bevat een expliciete proportionaliteitsbepaling: gegevens mogen uitsluitend naar aard en omvang worden verzameld voor het beoogde doel.

Dit betekent concreet dat verzoeken enkel betrekking mogen hebben op geïdentificeerde belastingplichtigen, dat generieke of preventieve gegevensverwerking verboden is, en dat alle informatieverzoeken schriftelijk gemotiveerd moeten zijn.

Het Kamerlid besluit dat Finland hiermee een strikt en begrensd systeem hanteert, in contrast met de Belgische praktijk, waar een veel bredere gegevensverwerking plaatsvindt.

Naast de Grondwet en de wet inzake belastingprocedures bestaat er een derde pijler: de wet op de belastingdienst zelf (*laki Verohallinnosta*⁸). Deze wet regelt de organisatie en bevoegdheden van de Finse Belastingdienst en bevat duidelijke bepalingen inzake gegevensbeheer.

Ten eerste geldt doelbinding: gegevens mogen uitsluitend worden gebruikt voor belastingheffing.

Ten tweede zijn er strikte bewaartermijnen: fiscale gegevens moeten na maximaal tien jaar worden vernietigd. Dit contrasteert sterk met de Belgische praktijk. In

loi formelle reprenant une description claire de l'objectif poursuivi et fixant des garanties.

Le membre souligne que le pouvoir judiciaire finlandais applique ce principe de manière stricte: un arrêté royal, un arrêté ministériel ou une circulaire ne suffisent pas pour satisfaire au principe de légalité.

Il renvoie à l'avis du Conseil d'État, selon lequel le traitement des données à caractère personnel doit reposer sur une base légale et ne peut pas être délégué. La loi doit en outre être suffisamment précise, ce qui est systématiquement respecté en Finlande, alors qu'en Belgique, on est beaucoup moins rigoureux à cet égard.

L'intervenant cite encore, outre la Constitution, la loi sur les procédures fiscales (*laki verotusmenettelystä*⁷). Cette loi définit les compétences de l'Administration fiscale finlandaise.

L'article 26 dispose que l'Administration fiscale (*Verhallinto*) peut uniquement demander les informations qui sont nécessaires pour procéder à une imposition correcte. La loi contient une disposition explicite relative à la proportionnalité: les données ne peuvent être collectées que si elles sont utiles à la réalisation de l'objectif visé. Cette exigence de proportionnalité doit s'apprécier en fonction de la nature des données et de leur quantité.

Cela signifie concrètement que les demandes ne peuvent concerner que des contribuables identifiés, que le traitement générique ou préventif des données est interdit, et que toutes les demandes d'information doivent être motivées par écrit.

Le membre conclut que la Finlande applique ainsi un système strict et balisé, contrairement à la Belgique, où le traitement des données est nettement plus étendu.

Outre la Constitution et la loi sur les procédures fiscales, il existe un troisième pilier: la loi sur l'Administration fiscale elle-même (*laki Verohallinnosta*⁸). Cette loi règle l'organisation et les compétences de l'Administration fiscale finlandaise et comprend des dispositions claires sur la gestion des données.

Premièrement, il y a un principe de finalité: les données ne peuvent être utilisées que pour l'imposition.

Deuxièmement, les délais de conservation sont stricts: les données fiscales doivent être détruites au bout de dix ans maximum, ce qui diffère fortement de la pratique

⁷ Laki verotusmenettelystä | 1558/1995 | Lainsäädäntö | Finlex.

⁸ Laki Verohallinnosta | 503/2010 | Lainsäädäntö | Finlex.

⁷ Laki verotusmenettelystä | 1558/1995 | Lainsäädäntö | Finlex.

⁸ Laki Verohallinnosta | 503/2010 | Lainsäädäntö | Finlex.

Finland worden gegevens na tien jaar vernietigd, terwijl in België de bewaartermijn formeel één jaar bedraagt, maar in de praktijk kan oplopen tot twintig à vijfentwintig jaar, aangezien deze pas ingaat na uitputting van alle procedures en betalingen.

Ten derde is gegevensuitwisseling enkel toegestaan met andere overheidsinstanties indien de wet dit expliciet toelaat.

Daarnaast voorziet de Finse wet in de aanstelling van een functionaris voor gegevensbescherming (*tietosuoja-vastaava*), vergelijkbaar met de Belgische Data Protection Officer (DPO). Deze houdt toezicht op de naleving van privacyregels. De spreker suggereert dat het nuttig zou zijn om ook de DPO van de FOD Financiën te horen.

Een vierde pijler is de Finse wet die de Europese anti-witwasrichtlijn omzet (*Laki rahanpesun ja terrorismin rahoittamisen estämisestä*) en financiële instellingen verplicht om cliënten te identificeren, transacties voortdurend te monitoren en verdachte transacties te melden aan de Financial Intelligence Unit (FIU), de Finse tegenhanger van de CFI. Artikel 6:3 van de voornoemde Finse wet luidt als volgt: “de op grond van deze wet verzamelde gegevens mogen niet worden gebruikt voor andere doeleinden dan de voorkoming en opsporing van witwassen of financiering van terrorisme”. Dit betekent een verbod op hergebruik, wat elke vorm van fiscale datamining of profilering uitsluit.

De vijfde en laatste tekst die het Finse systeem regelt is de wet op de gegevensbescherming (*Tietosuoja laki*), die uitvoering geeft aan de AVG en de kernbeginselen ervan bevestigt: rechtmatigheid, doelbinding, gegevens-minimalisatie, juistheid, bewaarbeperving, integriteit, vertrouwelijkheid en verantwoordingsplicht.

De Finse onafhankelijke gegevensbeschermingsautoriteit (*Tietosuoja valtuutetun toimisto*) heeft de bevoegdheid om toezicht te houden, boetes op te leggen en advies te geven aan het Parlement en de regering.

— Institutionele structuur

De spreker gaat vervolgens in op de institutionele structuur rondom de tegenhanger van het CAP in Finland en bij uitbreiding op het ontbreken van “*money control*”.

De Finse belastingadministratie (*Verohallinto*) is een autonome dienst verantwoordelijk voor de inning van alle

belge. En effet, le délai légal de conservation des données en Belgique est en principe d'un an, mais il peut atteindre en pratique vingt à vingt-cinq ans, car il ne commence à courir qu'après l'épuisement de toutes les procédures et lorsque tous les paiements ont été effectués.

Troisièmement, l'échange de données avec d'autres administrations publiques n'est autorisé que si la loi le permet explicitement.

Par ailleurs, la loi finlandaise prévoit la nomination d'un délégué à la protection des données (*tietosuoja vastaava*), comparable au *Data Protection Officer* (DPO) belge. Il est chargé de veiller au respect des règles en matière de protection de la vie privée. À cet égard, l'intervenant suggère qu'il serait utile d'entendre également le DPO du SPF Finances.

La loi finlandaise transposant la directive européenne anti-blanchiment (*Laki rahanpesun ja terrorismin rahoittamisen estämisestä*) est le quatrième pilier. Cette loi oblige les établissements financiers à identifier leurs clients, à surveiller en permanence leurs transactions et à signaler toute transaction suspecte à la Financial Intelligence Unit (FIU), le pendant finlandais de la CTIF. L'article 6:3 de la loi finlandaise précitée s'énonce comme suit: “les données recueillies en application de la présente loi ne peuvent être utilisées à d'autres fins que celles de prévenir ou de détecter des actes de blanchiment de capitaux et de financement du terrorisme”. (traduction) Cette loi implique donc une interdiction de réutilisation des données, ce qui exclut toute forme de *data mining* ou de profilage à des fins fiscales.

La loi sur la protection des données (*Tietosuoja laki*) est le cinquième et dernier pilier du système finlandais. Cette loi met en œuvre le RGPD et en confirme les principes fondamentaux: licéité, limitation des finalités, minimisation des données, exactitude, limitation de la conservation, intégrité, confidentialité et responsabilité.

L'autorité indépendante finlandaise chargée de la protection des données (*Tietosuoja valtuutetun toimisto*) est habilitée à exercer des contrôles, à infliger des amendes et à rendre des avis au Parlement et au gouvernement.

— Structure institutionnelle

L'intervenant aborde ensuite la structure institutionnelle encadrant le pendant du PCC en Finlande et réglant, par extension, l'absence de “*money control*”.

L'administration fiscale finlandaise (*Verohallinto*) est un service autonome chargé de percevoir tous les

ationale belastingen, het toezicht op de fiscale naleving en de uitvoering van internationale informatie-uitwisseling.

De Verohallinto beschikt over een geïntegreerd digitaal platform (www.vero.fi), maar heeft geen directe of permanente toegang tot bankrekeningen. Dat is vrij uniek. Op dat vlak geldt de stelregel “*open government, closed data*”.

Banken leveren jaarlijks enkel een beperkte dataset aan die door een afzonderlijke instantie wordt beheerd. Het betreft een soort inkomensregister. Elke bevraging van financiële instellingen gebeurt via een formeel verzoek, gekoppeld aan een individueel dossiernummer en onder tweevoudige interne controle. Er is zowel een operationele als een juridische toets.

Het inkomensregister (*Tulorekisteri*) is een nationaal register waarin werkgevers, pensioenfondsen en verzekeringsmaatschappijen realtime informatie aanleveren over inkomsten en sociale bijdragen. Toegepast op de Belgische Kruispuntbank Sociale Zekerheid (KSZ) zou dat betekenen dat deze databank tevens fiscale gegevens bevat. De inning van sociale bijdragen en achterstallige belastingen zou in België overigens ook beter door één instantie kunnen gebeuren. Dit zou de eenvoud, snelheid en kostprijs ten goede komen.

Het *Tulorekisteri* wordt beheerd door een onafhankelijke entiteit binnen de belastingdienst. De toegang is strikt gereguleerd: alleen instanties die een wettelijke taak hebben, zoals sociale zekerheidsinstellingen, de belastingdienst of pensioenfondsen, kunnen gegevens opvragen en enkel binnen hun bevoegdheden. De banken hebben opvallend genoeg geen toegang tot het register.

De Finanssivalvonta houdt toezicht op deze regels en op de financiële sector. De toezichthouder staat zelf onder het toezicht van de Nationale Bank van Finland. Ze waakt over de naleving van de anti-witwas- en de financiële transactieregels, en kan sancties opleggen bij nalatigheid. De *Finanssivalvonta* deelt echter geen individuele klantgegevens met de belastingdienst en samenwerking gebeurt uitsluitend op geaggregeerd of geanonimiseerd niveau. In tegenstelling tot pseudonymisering houdt dit geen risico op identificatie in.

Een volgende instelling is de Financial Intelligence Unit (FIU), zoals reeds vermeld de Finse tegenhanger

impôts nationaux, de contrôler le respect des obligations fiscales et de mettre en œuvre l'échange international d'informations.

Elle dispose d'une plateforme numérique intégrée (www.vero.fi), mais n'a pas d'accès direct ou permanent aux comptes bancaires, ce qui en fait une institution plutôt unique, puisque le principe “*open government, closed data*” prévaut dans ce domaine.

Les banques ne communiquent chaque année qu'un ensemble limité de données qui sont gérées par un organisme distinct. Il s'agit d'une sorte de registre des revenus. Toute consultation auprès des établissements financiers fait l'objet d'une demande formelle, rattachée à un numéro de dossier individuel et soumise à un double contrôle interne – à la fois opérationnel et juridique.

Le registre des revenus (*Tulorekisteri*) est un registre national dans lequel les employeurs, les fonds de pension et les compagnies d'assurance transmettent des informations en temps réel sur les revenus et les cotisations sociales. Si l'on appliquait sa structure à la Banque-Carrefour belge de la sécurité sociale (BCSS), cette banque de données contiendrait par conséquent aussi des données fiscales. La perception des cotisations sociales et des arriérés d'impôts pourrait d'ailleurs être confiée en Belgique à une seule instance dans un souci de simplicité, de rapidité et de rentabilité.

Le registre précité est géré en Finlande par une entité indépendante au sein de l'administration fiscale. Son accès est strictement réglementé: seules les instances poursuivant une mission légale, notamment les organismes de sécurité sociale, l'administration fiscale ou les fonds de pension, peuvent consulter les données qui y sont enregistrées, et uniquement dans le cadre de leurs compétences. Il convient de souligner que les banques n'ont pas accès à ce registre.

L'Autorité finlandaise de surveillance financière (*Finanssivalvonta*) supervise le respect de ces règles et assure la surveillance du secteur financier. Elle est elle-même placée sous la tutelle de la Banque nationale de Finlande. Elle veille au respect des règles applicables à la lutte contre le blanchiment et aux transactions financières, et peut imposer des sanctions en cas de manquement. L'autorité finlandaise précitée ne partage toutefois aucune donnée individuelle de ses clients avec l'administration fiscale et toute coopération a lieu à un niveau agrégé ou anonymisé. Contrairement à la pseudonymisation, ces procédures ne comportent aucun risque d'identification.

La Financial Intelligence Unit (FIU) est une autre institution que l'intervenant souhaiterait évoquer. Comme

van de Cel voor Financiële Informatieverwerking (CFI), die deel uitmaakt van de centrale politie in Finland en meldingen ontvangt van verdachte transacties. Deze worden verder onderzocht onder het toezicht van het openbaar ministerie.

Ter vergelijking: de Belgische regeling houdt in dat banken verdachte transacties melden aan de CFI. Wanneer uit hun onderzoek blijkt dat er mogelijk fraude in het spel is, wordt de zaak overgedragen aan het parket. In Finland is dat enigszins anders: de FIU kan enkel gegevens delen met de belastingadministratie in het kader van een lopend onderzoek en mits gerechtelijke toestemming. Er bestaat geen permanente gegevensstroom tussen de FIU in Finland en de fiscus, zoals het Belgische “*money control*” dat zou voorzien.

Verder beschikt de Finse gegevensbeschermingsautoriteit (Tietosuojavaltuutetun toimisto), de nationale toezichthouder, over onderzoeksbevoegdheden, het recht om inspecties uit te voeren bij overheidsdiensten en de bevoegdheid om administratieve geldboetes tot 1 miljoen euro op te leggen voor de overheid.

Deze autoriteit geldt als een volwassen en volledig ontwikkelde toezichthouder en zou als model moeten fungeren voor de tandeloze Belgische GBA, wier machteloosheid wordt geïllustreerd in het debat over de voorliggende wetgeving: ondanks een uiterst negatief advies heeft de instelling niet de bevoegdheid om tussen te komen of om boetes op te leggen, in tegenstelling tot haar Finse tegenhanger.

De *Tietosuojavaltuutetun toimisto* rapporteert jaarlijks aan het Finse Parlement over de naleving van de privacywetgeving. In het verslag van 2022 staat dat het fiscaal databaseer in Finland conform de beginselen van proportionaliteit en transparantie verloopt en dat er geen aanwijzingen zijn van structurele profilering of algoritmische besluitvorming. Dit staat in schril contrast met het negatieve advies van de GBA over het voorliggende wetsontwerp.

— Gegevensstromen

De heer Van Quickenborne gaat vervolgens in op de gegevensstromen en de wettelijke bevoegdheden dienaangaande in Finland.

indiqué précédemment, celle-ci est le pendant finlandais de la Cellule de traitement des informations financières (CTIF). Elle fait partie de la police centrale en Finlande et reçoit les signalements de transactions suspectes. Ceux-ci font l'objet d'une enquête approfondie sous la supervision du ministère public.

À titre de comparaison, les banques sont tenues, en application de la réglementation belge, de signaler les transactions suspectes à la CTIF. Si l'enquête menée par celle-ci révèle l'existence d'une possible fraude, l'affaire est transmise au parquet. En Finlande, la procédure est quelque peu différente: la FIU ne peut partager des informations avec l'administration fiscale que dans le cadre d'une enquête en cours et moyennant une autorisation judiciaire. Des informations ne sont donc pas échangées en permanence entre la FIU et le fisc finlandais, comme le prévoirait le système belge de “*money control*”.

Par ailleurs, l'autorité finlandaise chargée de la protection des données (Tietosuojavaltuutetun toimisto), à savoir l'autorité nationale de contrôle, dispose de pouvoirs d'enquête, du droit de procéder à des inspections auprès des services publics et de la compétence d'infliger des amendes administratives – pouvant aller jusqu'à un million d'euros – aux pouvoirs publics.

Cette autorité est considérée comme un organisme de contrôle à part entière et pleinement abouti et devrait servir de modèle à l'APD, dont l'impuissance s'illustre dans le débat sur la législation en projet: malgré un avis extrêmement négatif, l'APD n'est pas habilitée à intervenir ni à infliger des amendes, contrairement à son pendant finlandais.

Chaque année, l'autorité finlandaise chargée de la protection des données fait rapport au Parlement du respect de la législation en matière de protection de la vie privée. Le rapport de 2022 indique que la gestion des données fiscales en Finlande est conforme aux principes de proportionnalité et de transparence et que rien n'indique l'existence d'un profilage structurel ni d'une prise de décisions automatisée (recours à des algorithmes). Ce rapport contraste nettement avec l'avis négatif rendu par l'APD au sujet du projet de loi à l'examen.

— Flux de données

M. Van Quickenborne aborde ensuite la question des flux de données et des compétences légales y afférentes en Finlande.

1. Routinegegevens

Financiële instellingen sturen jaarlijks een beperkte dataset naar de Verohallinto. De volgende gegevens worden overgemaakt:

— De totaalbedragen van ontvangen rente en dividenden. Dit gaat verder dan in België, waar de praktijk van de bevrijdende roerende voorheffing geldt, al zal de toekomstige wetgeving inzake meerwaardebelasting een en ander wijzigen wat de aangifte van dividenden betreft.

— De waarde van bepaalde effectenportefeuilles.

— De hypotheekinformatie voor aftrekdoeleinden, wat in België eveneens gebeurt.

De Finse praktijk vloeit voort uit de keuze om sterk in te zetten op vooraf ingevulde belastingaangiften, en is vergelijkbaar met het Zweedse systeem.

2. Ad-hocbevragingen

Wanneer er aanwijzingen zijn van een onjuiste aangifte of van fiscale fraude kan de belastingdienst specifieke informatie opvragen bij een bank of een derde partij.

Deze procedure dient aan vier voorwaarden te voldoen: schriftelijke motivering, verwijzing naar het relevante wetsartikel, interne goedkeuring door een afdelingshoofd en registratie in het toezichtlogboek.

De reglementering is bijgevolg strenger dan de huidige Belgische, waarbij het lid opmerkt dat “*money control*” nog verder gaat en hoegenaamd geen toezicht voorziet. Elke bevraging van de Finse administratie wordt automatisch gelogd en kan later worden gecontroleerd door een parlementair controlecomité.

De heer Van Quickenborne verwijst naar een voorstel van de heer Michel Maus (hoogleraar fiscaal recht, VUB) die in *De Morgen* van 18 november 2025 vraagtekens plaatst bij de proportionaliteit van de door de minister voorgestelde maatregel. De heer Maus pleit voor een “Comité F”, met onafhankelijk toezicht op de bevraging van het CAP.

Finland heeft daarnaast – in tegenstelling tot Duitsland, Frankrijk of België – geen nationaal bankregister. Banken bewaren hun eigen klantgegevens en zijn alleen verplicht om mee te werken bij specifieke gemotiveerde verzoeken. Er bestaat geen centrale toegang voor de fiscus of politie, en geen geautomatiseerde koppeling tussen fiscale en bancaire databanken.

1. Données de routine

Les institutions finlandaises envoient chaque année, à la Verohallinto, un échantillon limité de données comportant les données suivantes:

— Les totaux des intérêts et des dividendes perçus. Ces données vont plus loin qu’en Belgique, où la pratique du précompte mobilier libératoire est d’application, même si la future législation relative à la taxe sur les plus-values modifiera certaines dispositions de la déclaration des dividendes.

— La valeur de certains portefeuilles de titres.

— Les informations relatives aux hypothèques à des fins de déduction, comme en Belgique.

La pratique finlandaise découle du choix d’investir fortement dans les déclarations fiscales préremplies, et elle est comparable au système suédois.

2. Consultations ad hoc

En cas d’indices de déclaration erronée ou de fraude fiscale, l’administration fiscale peut demander des informations spécifiques à une banque ou à un tiers.

Cette procédure doit satisfaire à quatre conditions: motivation écrite, renvoi à l’article de loi pertinent, approbation interne par un chef de service et enregistrement dans le registre de contrôle.

La réglementation finlandaise est donc plus stricte que la réglementation belge actuelle, l’intervenant ajoutant à ce propos que le “*money control*” ira encore plus loin et qu’il ne prévoit absolument aucun contrôle. Chaque consultation de l’administration finlandaise est automatiquement enregistrée et peut être ultérieurement contrôlée par une commission de contrôle parlementaire.

M. Van Quickenborne renvoie à une proposition de M. Michel Maus (professeur de droit fiscal à la VUB) qui, dans l’édition du *Morgen* du 18 novembre 2025, s’interroge sur la proportionnalité de la mesure proposée par le ministre. M. Maus plaide en faveur d’un “Comité F” qui contrôlerait les consultations du PCC en toute indépendance.

Contrairement à l’Allemagne, à la France ou à la Belgique, la Finlande ne dispose en outre pas d’un registre bancaire national. Les banques conservent leurs propres données concernant leurs clients, et elles ne sont tenues de coopérer qu’en cas de demandes spécifiques motivées. La Finlande n’a prévu ni accès centralisé pour le fisc ou la police, ni couplage automatisé entre les banques de données fiscales et bancaires.

3. Logging en toezicht

In Finland wordt elke gegevensopvraging door de overheid geregistreerd in een beveiligd logboek. Daarin wordt de identiteit van de ambtenaar opgenomen, met daarnaast de juridische basis van de handeling, datum en tijdstip van de toegang en ten slotte het betrokken dossier. De logs kunnen worden gecontroleerd door de interne auditdienst van de Finse belastingdienst, door de autoriteit voor gegevensbescherming en indien nodig ook door het Finse parlement.

De logs worden vijf jaar bewaard, terwijl deze termijn in België slechts zes maanden bedraagt. Als de minister zoals hij beweert daadwerkelijk het vertrouwen van de fiscus in de belastingplichtigen wil vergroten, zou hij deze termijn kunnen verlengen en zorgen voor een kennisgevingsplicht.

— De constitutionele en Europese context

Wat de constitutionele proportionaliteit betreft, beschermt artikel 10 van de Finse Grondwet niet alleen het privéleven, maar verplicht het de wetgever ook tot nauwkeurige afbakening van privacy-inmenging. Er gelden drie cumulatieve voorwaarden: de inmenging moet noodzakelijk en proportioneel zijn, en ze moet voorzien zijn in een formele wet. De wetgever past die voorwaarden strikt toe op elke uitbreiding van bevoegdheden in het domein van fiscaliteit en politie.

De spreker gaat vervolgens in op het Europese kader en de rechtspraak die voor Finland relevant is. Finland volgt consequent de rechterlijke uitspraken van het EHRM en van het Europees Hof van Justitie. In parlementaire adviezen worden onder meer het *Digital Rights Ireland* en het *Tele2 Sverige*-arrest expliciet geïncorporeerd. Dit houdt in dat algemene ongedifferentieerde gegevensverzameling grondwettelijk verboden is. Ook *La Quadrature du Net* is voor Finland een bindend, richtinggevend arrest voor alle nationale wetgeving.

Daarnaast bestaat er parlementaire controle. Het Finse Parlement speelt een actieve rol op het vlak van gegevensbescherming. Het zou interessant zijn om daarover van gedachten te wisselen met de Finse tegenhanger van de commissie voor Financiën en Begroting.

De commissie van het Finse Parlement bevoegd voor de Grondwet beoordeelt alle wetsontwerpen op grondwettelijke compatibiliteit. Dit gebeurde bijvoorbeeld voor de omzetting van de AVG, waarbij het advies luidde dat de bescherming van persoonsgegevens behoort tot de kern van de Finse rechtsstaat. De commissie voor Financiën en Begroting zou dit voorbeeld kunnen volgen en advies vragen aan de Kamercommissie Grondwet

3. Enregistrement et contrôle

En Finlande, chaque consultation de données par les pouvoirs publics est enregistrée dans un journal sécurisé. Celui-ci mentionne l'identité de l'agent du fisc, ainsi que la base juridique de l'acte, la date et l'heure de l'accès et enfin le dossier concerné. Les journaux informatiques (*logs*) peuvent être contrôlés par le service d'audit interne de l'administration fiscale finlandaise, par l'autorité chargée de la protection des données et, au besoin, par le Parlement finlandais également.

Les journaux informatiques (*logs*) sont conservés durant cinq ans, tandis que ce délai n'est que de six mois en Belgique. Si, comme il l'affirme, le ministre souhaite réellement renforcer la confiance des contribuables envers le fisc, il pourrait prolonger ce délai et prévoir une obligation de notification.

— Contexte constitutionnel et européen

S'agissant de la proportionnalité constitutionnelle, l'article 10 de la Constitution finlandaise protège la vie privée, mais oblige en outre le législateur à délimiter avec précision l'ingérence dans la vie privée. Trois conditions cumulatives sont prévues: l'ingérence doit être nécessaire, proportionnée, et fondée sur une loi formelle. Le législateur applique strictement ces conditions à toute extension des compétences dans le domaine de la fiscalité et de la police.

L'intervenant aborde ensuite le cadre européen et la jurisprudence pertinente pour la Finlande, qui se conforme systématiquement aux arrêts rendus par la Cour européenne des droits de l'homme et par la Cour de justice de l'Union européenne. Les avis parlementaires intègrent explicitement, entre autres, les arrêts *Digital Rights Ireland* et *Tele2 Sverige*. Cela signifie que la collecte généralisée et indifférenciée de données est interdite par la Constitution. L'arrêt "*La Quadrature du Net*" est également contraignant pour la Finlande et a valeur de référence pour toute la législation nationale.

Un contrôle parlementaire est en outre exercé. Le Parlement finlandais joue un rôle actif dans le domaine de la protection des données. Il serait intéressant de procéder à un échange de vues à ce sujet avec le pendant finlandais de la commission des Finances et du Budget.

La commission du Parlement finlandais compétente pour la Constitution évalue la compatibilité constitutionnelle de tous les projets de loi. Ce fut le cas, par exemple, pour la transposition du RGPD. L'avis y afférent indique que la protection des données à caractère personnel est au cœur de l'État de droit finlandais. La commission des Finances et du Budget pourrait suivre cet exemple et demander que la commission de la Constitution et

en Institutionele Vernieuwing met betrekking tot het voorliggende *amendement nr. 16* (DOC 56 0963/005) van de regering.

Het Finse Parlement controleert daarnaast ook de uitvoering van de anti-witwaswetten en de fiscale procedures via jaarlijkse hoorzittingen met de minister van Financiën en de directeur van de belastingdienst.

— *Hoofdkenmerken en werking van het Finse systeem*

De Finse rechtsstatelijke infrastructuur kan in vier belangrijke kenmerken worden samengevat.

1. Strikte legaliteit

Elk onderdeel van het systeem berust op een formele wet met een duidelijke doelomschrijving. In de voorliggende teksten van de regering is dat volstrekt niet het geval.

2. Geen centraal register

Er kunnen enkel ad hoc opvragingen gebeuren met menselijke goedkeuring.

3. Onafhankelijk toezicht

Toezicht gebeurt door de Finse autoriteit voor gegevensbescherming, door het Finse parlement en via interne audits.

4. Proportionaliteit en vertrouwen

De fiscale regelgeving wordt zeer goed nageleefd (in tegenstelling tot in België), en dat zonder massale surveillance.

Efficiëntie is in Finland niet afhankelijk van datavolume, maar van juridische precisie en institutionele discipline. Het contrast met België, waar verregaande digitale observatie van gegevens wordt gepland, is groot.

Kan de minister in dat verband aangeven hoeveel individuele gegevens het CAP precies bevat? Volgens de berekening van de spreker zouden het er 330 miljoen zijn.

België vertrouwt op algoritmische screening en datamining. Finland kiest daarentegen voor een juridisch geconditioneerde datahuishouding: de overheid vertrouwt haar burgers in plaats van het vertrouwen te ondermijnen.

De heer Van Quickenborne vervolgt met een schets van de feitelijke werking van het Finse systeem. Hoe worden gegevens concreet uitgewisseld? Hoe worden

du Renouveau institutionnel de la Chambre rende un avis sur l'*amendement n° 16* (DOC 56 0963/005) du gouvernement.

Le Parlement finlandais contrôle en outre la mise en œuvre des lois anti-blanchiment et des procédures fiscales par le biais d'auditions annuelles du ministre des Finances et du directeur de l'administration fiscale.

— *Principales caractéristiques et fonctionnement du système finlandais*

En résumé, l'infrastructure de l'État de droit finlandais a quatre caractéristiques principales:

1. Légalité stricte

Chaque élément du système s'appuie sur une loi formelle dont l'objectif est clairement défini. Ce n'est absolument pas le cas dans les textes du gouvernement à l'examen.

2. Pas de registre central

Seules des consultations *ad hoc* soumises à une approbation humaine peuvent avoir lieu.

3. Contrôle indépendant

Le contrôle est assuré par l'autorité finlandaise chargée de la protection des données, par le Parlement finlandais et par des audits internes.

4. Proportionnalité et confiance

La réglementation fiscale est respectée scrupuleusement (ce n'est pas le cas en Belgique), sans surveillance massive.

En Finlande, l'efficacité ne dépend pas du volume de données, mais de la précision juridique et de la discipline institutionnelle. Le contraste avec la Belgique, où une surveillance numérique approfondie des données est prévue, est considérable.

À cet égard, le ministre peut-il indiquer le nombre de données individuelles que le PCC contient exactement? Selon les calculs de l'intervenant, il s'agirait de 330 millions de données.

La Belgique table sur un filtrage algorithmique et sur le *data mining*. La Finlande, en revanche, opte pour une gestion des données conditionnée par la loi, c'est-à-dire que les pouvoirs publics font confiance à leurs citoyens au lieu de saper leur confiance.

M. Van Quickenborne poursuit en dépeignant le fonctionnement concret du système finlandais. Comment l'échange des données se déroule-t-il concrètement?

burgers beschermd tegen misbruik? Hoe worden controle en vertrouwen in balans gehouden?

In het Finse model is het verzamelen van informatie geen doel op zich. Als de overheid gegevens verwerkt kan dat enkel met duidelijk omschreven doeleinden. Een aanvaardbare concrete doelstelling is bijvoorbeeld de bestrijding van btw-carousels, georganiseerde fraude en witwassen. In het voorliggende amendement nr. 16 is echter enkel sprake van “een risico tot het plegen van een inbreuk op een wet of een reglementering waarvan de toepassing behoort tot de opdrachten van de Federale Overheidsdienst Financiën”. Een dergelijke doelstelling gaat veel te ver. De Belgische evolutie van het CAP naar “*money control*”, waarbij de overheid structureel toegang krijgt tot alle bankrekeningen, is in Finland juridisch ondenkbaar.

De praktische werkwijze verschilt daarnaast fundamenteel van de plannen van de minister. Finse financiële instellingen sturen jaarlijks gegevens door naar de belastingadministratie via sterk beveiligde elektronische kanalen. Deze data worden gebruikt voor de vooraf ingevulde belastingaangifte. Burgers ontvangen deze reeds in maart; in België duurt dat tot mei of juni. De Finse belastingadministratie gebruikt die gegevens uitsluitend ter verificatie van de door de belastingplichtige versterkte informatie. Er is geen permanente monitoring van transacties noch van saldi.

Indien de fiscus vermoedt dat een aangifte onjuist is, dient zij zich met een gericht informatieverzoek te wenden tot de financiële instelling. De bank is verplicht om te antwoorden, maar mag weigeren als het verzoek niet proportioneel of onvoldoende gemotiveerd is. Dat is een verschil met het CAP, waar de NBB niet kan weigeren te antwoorden op vragen. De Finse belastingdienst kan echter wel naar de bestuursrechter stappen, die dan binnen enkele dagen een uitspraak doet.

Menselijke tussenkomst is in Finland structureel ingebouwd. Geautomatiseerde bulkopvragingen, zoals de minister voorstelt, zijn uitgesloten.

Het inkomensregister werd in 2019 ingevoerd. Het bevat een belangrijk innovatief en uniek element, namelijk realtime informatie over lonen en sociale bijdragen, aangeleverd door werkgevers. In België is dat evenmin het geval.

Critici zullen opwerpen dat dit Finse inkomensregister klaarblijkelijk zeer veel informatie bevat over inkomens, sociale bijdragen en belastingen. Het is echter geen fiscaal toezichtinstrument: de belastingdienst gebruikt

Comment les citoyens sont-ils protégés contre les abus? Comment le juste équilibre entre contrôle et confiance est-il assuré?

Dans le modèle finlandais, la collecte de données n'est pas une fin en soi. Lorsque les autorités traitent des données, c'est uniquement en poursuivant des objectifs clairement définis. Un objectif concret acceptable sera par exemple la lutte contre les carousels à la TVA, la fraude organisée et le blanchiment. L'amendement n° 16 à l'examen évoque en revanche uniquement “un risque de commission d'une infraction à une loi ou à une réglementation dont l'application relève des missions du Service public fédéral Finances”. Cet objectif va beaucoup trop loin. L'évolution qui veut qu'en Belgique, le PCC se mue en “*money control*”, les pouvoirs publics obtenant ainsi un accès structurel à l'ensemble des comptes bancaires, est impensable sous l'angle juridique finlandais.

La méthode pratique diffère en outre fondamentalement des projets du ministre. Chaque année, les établissements financiers finlandais transmettent des données à l'administration fiscale par des canaux électroniques hautement sécurisés. Ces données sont utilisées pour la déclaration fiscale préremplie. Les citoyens la reçoivent dès le mois de mars, tandis qu'en Belgique, les citoyens doivent attendre jusqu'en mai ou en juin. L'administration fiscale finlandaise utilise ces données exclusivement pour vérifier les informations fournies par le contribuable. Il n'y a pas de surveillance permanente des transactions, ni des soldes.

Si le fisc soupçonne une déclaration d'être inexacte, il doit adresser une demande d'information ciblée à l'établissement financier. La banque est tenue d'y répondre, mais elle peut la refuser si la demande n'est pas proportionnée ou suffisamment motivée. C'est une différence par rapport au PCC, puisque la BNB ne peut pas, quant à elle, refuser de répondre aux questions. Le fisc finlandais peut toutefois saisir le juge administratif, qui se prononcera dans un délai de quelques jours.

En Finlande, l'intervention humaine est intégrée structurellement. Les demandes en masse automatisées que propose le ministre y sont exclues.

Le registre des revenus a été instauré en 2019. Il comporte un élément novateur et unique majeur, à savoir des informations en temps réel sur les rémunérations et les cotisations sociales fournies par les employeurs. En Belgique, ce n'est pas le cas non plus.

Les détracteurs objecteront que ce registre finlandais contient manifestement une mine d'informations sur les revenus, les cotisations sociales et les impôts. Il ne s'agit toutefois pas d'un instrument de contrôle fiscal: le

het enkel voor de voorbereiding van de automatische aangifte, terwijl andere instellingen zoals pensioenfondsen uitsluitend binnen hun respectieve wettelijke taken toegang hebben. Elke instantie heeft een toegangsprofiel en mag enkel de voor haar bevoegdheid relevante velden raadplegen. In het CAP is dat niet het geval: informatiegerechtigden krijgen alle informatie betreffende een bepaalde persoon. Ze mogen weliswaar alleen de voor hen toegelaten zaken consulteren, maar daarvoor moet je uitgaan van hun goede trouw. Het is opnieuw een fundamenteel verschil tussen beide landen.

Finland koppelt digitalisering aan zogenaamde wettelijke segmentering, een technische verankering van het proportionaliteitsbeginsel. Dat zou in België ook moeten gebeuren. De spreker verwijst naar zijn amendement nr. 60 (DOC 56 0963/009).

— Dossierselectie

Wat betreft het gebruik van gegevens en algoritmen in Finland, gaat de spreker vooreerst in op de selectie van dossiers.

Voor de controle van fiscale gegevens steunt de Finse belastingadministratie ten eerste uitsluitend op fiscaal beschikbare data. Statistische analyse vindt plaats om aangiften met een verhoogd risico op fouten te selecteren. Statistische analyse op bankgegevens is niet toegelaten. De doelstelling is fundamenteel anders dan in de voorliggende plannen van de minister: het oogmerk is om de efficiëntie te verhogen, niet om burgers te profileren. Een richtlijn bepaalt dat elk risicosignaal manueel moet worden beoordeeld voordat een controle wordt geopend. De verantwoordelijke ambtenaar noteert zijn motivatie in het dossier en dit document is toegankelijk voor interne audit en ook voor de Finse gegevensbeschermingsautoriteit.

Bovendien vindt er in Finland geen datamining plaats: automatische risicoprofilering is zonder meer verboden. De Finse autoriteit voor gegevensbescherming verklaart in een rapport uit 2021 dat het gebruik van algoritmen ter identificatie van potentiële fraudeurs zonder individuele noodzaak in strijd is met artikel 22 van de AVG en met artikel 10 van de Finse Grondwet.

De belastingdienst mag wel datasets analyseren voor beleids- of onderzoeksevaluaties, maar niet voor individuele dossiers. Finland kiest voor dataminimalisatie in plaats van “*predictive analytics*”.

fisc ne l'utilise que pour préparer la déclaration automatique, alors que d'autres institutions, comme les fonds de pension n'y ont accès que dans les limites de leurs missions légales respectives. Chaque instance dispose d'un profil d'accès et ne peut consulter que les champs qui relèvent de ses compétences. Ce n'est pas le cas en ce qui concerne le PCC: les demandeurs d'informations reçoivent toutes les informations concernant une personne précise. Certes, ils ne peuvent consulter que les éléments qui leur sont autorisés, mais ce modèle suppose leur bonne foi. Il s'agit de nouveau d'une différence fondamentale entre les deux pays.

La Finlande subordonne la numérisation à une “segmentation légale”, qui constitue un ancrage technique du principe de proportionnalité. Cela devrait également être le cas en Belgique. L'intervenant renvoie à son amendement n° 60 (DOC 56 0963/009).

— Sélection des dossiers

S'agissant de l'utilisation des données et des algorithmes en Finlande, l'intervenant se penche d'abord sur la sélection des dossiers.

Pour contrôler les données fiscales, l'administration fiscale finlandaise s'appuie tout d'abord sur les données fiscales disponibles, exclusivement. Une analyse statistique est effectuée afin de sélectionner les déclarations présentant un risque accru d'erreurs. L'analyse statistique des données bancaires n'est pas autorisée. L'objectif diffère fondamentalement de ceux des projets à l'examen du ministre: le but est d'accroître l'efficacité, et non pas de profiler les citoyens. Une directive dispose que chaque signal de risque doit être évalué manuellement avant l'ouverture d'un contrôle. Le fonctionnaire responsable consigne sa justification dans le dossier, un document qui peut être consulté pour un audit interne et par l'autorité finlandaise de protection des données.

De plus, il n'y a pas de *data mining* en Finlande: le profilage automatique des risques est tout bonnement interdit. L'autorité finlandaise de protection des données déclare, dans un rapport de 2021, que l'utilisation d'algorithmes pour identifier des fraudeurs potentiels sans nécessité individuelle est contraire à l'article 22 du RGPD et à l'article 10 de la Constitution finlandaise.

Le fisc peut toutefois analyser des séries de données pour mener des évaluations à des fins de stratégie et de recherche, mais pas pour des dossiers individuels. La Finlande opte pour la minimalisation des données en lieu et place des analyses prédictives (*predictive analytics*).

— Rechtsbescherming van burgers in Finland

1. Inzagerecht en kennisgeving

Iedere burger heeft recht op inzage in zijn dossier op grond van artikel 16 van de Finse wet inzake openbaarheid van bestuur en op grond van artikel 15 van de AVG.

Een verschil tussen België en Finland is dat de betrokkenen in Finland achteraf moeten worden geïnformeerd wanneer de fiscus gegevens opvraagt bij derden. De kennisgevingsplicht houdt in dat de overheid burgers proactief dient te informeren over vier elementen: de gegevens die zijn opgevraagd, bij welke instelling, op welke wettelijke basis en op welke datum. De kennisgeving kan tijdelijk worden uitgesteld tijdens een lopend onderzoek, maar is verplicht zodra dat is afgerond. De transparantieplicht maakt onrechtmatige bevragingen praktisch onmogelijk.

Deze kennisgevingsplicht zorgt ervoor dat het systeem functioneert. Het veronderstelt vertrouwen van de administratie in de burger, waardoor ook het vertrouwen van diezelfde burger in de overheid toeneemt. Deze deugdzame cirkel leidt ertoe dat de regels gerespecteerd worden.

2. Bezwaar en beroep

Naast inzagerecht en kennisgeving, bestaat er een bezwaar- en beroepsprocedure. De burger kan tegen elke fiscale beslissing bezwaar indienen. Indien dit wordt verworpen, kan beroep worden aangetekend. Sommige commissieleden zullen opwerpen dat wie niet akkoord gaat met de administratie ook in België naar de rechtbank kan stappen. Het verschil is echter dat de Finse rechtbank niet alleen de inhoud van een dossier of van een belastingaanslag toetst, maar ook de wettigheid van de gegevensverwerking. In België heeft de rechtbank die bevoegdheid niet.

De heer Van Quickenborne verwijst naar een uitspraak van de hoogste Finse bestuursrechtbank. In 2018 werd over een belastingonderzoek waarbij bankgegevens zonder voorafgaande motivering waren opgevraagd geoordeeld dat dit een ontoelaatbare inbreuk op artikel 10 van de Grondwet vormde.

3. Schadevergoeding en tuchtrecht

Artikel 82 van de AVG voorziet dat EU-burgers recht hebben op een schadevergoeding indien de privacy op fiscaal vlak onrechtmatig wordt geschonden. Kan de minister toelichten hoe deze bepaling in België in fiscale zaken wordt toegepast?

— Protection juridique des citoyens en Finlande

1. Droit d'accès et notification

Chaque citoyen a le droit de consulter son dossier sur la base de l'article 16 de la loi finlandaise relative à la publicité de l'administration et de l'article 15 du RGPD.

Une différence par rapport à la Belgique est qu'en Finlande, les intéressés doivent être informés *a posteriori* des demandes de données que le fisc adresse à des tiers. L'obligation de notification implique que les pouvoirs publics doivent informer proactivement les citoyens de quatre éléments: les données qui ont été demandées, l'institution auprès de laquelle elles l'ont été, sur quelle base légale et à quelle date. La notification peut être temporairement différée pendant une enquête en cours, mais elle est obligatoire dès que celle-ci est terminée. L'obligation de transparence a pour effet de rendre les demandes illégales pratiquement impossibles.

Cette obligation de notification garantit le fonctionnement du système. Elle suppose la confiance de l'administration envers le citoyen, ce qui accroît également la confiance de ce dernier envers l'autorité. Ce cercle vertueux conduit au respect des règles.

2. Réclamation et recours

Outre le droit d'accès et la notification, il existe une procédure de réclamation et de recours. Le citoyen peut introduire une réclamation contre toute décision fiscale. Si cette réclamation est rejetée, un recours peut être introduit. Certains membres de la commission feront valoir qu'en Belgique, le contribuable qui est en désaccord avec l'administration peut également saisir le tribunal. La différence est toutefois que le tribunal finlandais contrôle non seulement le contenu d'un dossier ou d'un avis d'imposition, mais aussi la légalité du traitement des données. En Belgique, le tribunal n'est pas compétent à cet effet.

M. Van Quickenborne renvoie à une décision rendue par la plus haute juridiction administrative finlandaise. En 2018, celle-ci a considéré qu'une enquête fiscale, dans le cadre de laquelle des données bancaires avaient été demandées sans motivation préalable, avait porté atteinte de manière inadmissible à l'article 10 de la Constitution.

3. Indemnisation et droit disciplinaire

Selon l'article 82 du RGPD, les citoyens de l'Union européenne ont droit à une indemnisation en cas d'atteinte illégitime à leur vie privée dans le cadre d'une procédure fiscale. Le ministre peut-il préciser comment cette disposition est appliquée en Belgique en matière fiscale?

Daarnaast kan de Finse toezichhouder voor de privacy-bescherming tevens tuchtrechtelijke stappen nemen tegen ambtenaren die wetsovertredingen begaan. In België is een dergelijke unieke bepaling volstrekt uitgesloten.

Deze combinatie van civielrechtelijke en administratieve sancties garandeert de preventieve werking van het systeem. Finse burgers hebben solide rechten.

In het voorliggende amendement nr. 16 is niets van dit alles terug te vinden: van kennisgeving, inzagerecht, een bezwaar- en beroepsprocedure of een schadevergoeding is geen sprake, laat staan van tuchtrecht.

4. Toezicht en verantwoordingsplicht

Het is één zaak is om de rechten van burgers te beschermen (waarbij de betrokkenen zelf proactief stappen moeten zetten), een andere zaak is de manier waarop het toezicht en de verantwoordingsplicht worden georganiseerd. Ook op dat vlak is Finland opnieuw uniek: de Finse autoriteit voor gegevensbescherming voert jaarlijks controles uit op de Finse belastingdienst.

In 2022 heeft deze autoriteit geoordeeld dat de Finse belastingadministratie voldoet aan de AVG-vereisen inzake proportionaliteit, doelbinding en bewaartermijnen, en dat de loggingsystemen de individuele verantwoordelijkheid van ambtenaren garanderen.

Kan de minister laten weten of de GBA dergelijke controles uitvoert op de Belgische fiscus? Is dat vergelijkbaar met het Finse systeem? Wat zijn de conclusies die daaruit voortvloeien? Is remediëring noodzakelijk?

Het systeem in Finland werkt weliswaar niet helemaal perfect: zo werd aanbevolen om de kennisgeving aan burgers sneller te verzenden en om interne opleidingen over dataminimalisatie te intensifiëren. Kennisgeving is in België alvast onbestaande, tenzij de betrokkene erom vraagt. Kan de minister toelichten of er interne opleidingen voor dataminimalisatie bestaan bij de FOD Financiën in het kader van CAP (en in de toekomst ook "*money control*")?

Een tweede vorm van toezicht gebeurt door twee commissies in het Finse Parlement (bevoegd voor de toetsing aan de Grondwet en voor de begrotingscontrole) die waken over de Finse tegenhanger van het CAP: de commissies.

En outre, l'autorité finlandaise de protection de la vie privée peut également engager des procédures disciplinaires à l'encontre des fonctionnaires qui enfreignent des dispositions légales. En Belgique, une disposition unique de ce type est totalement exclue.

Cette combinaison de sanctions civiles et administratives garantit l'effet préventif du système. Les citoyens finlandais disposent de droits solides.

L'amendement n° 16 à l'examen ne comporte aucun élément similaire: il n'y est nullement question de notification, de droit d'accès ou de procédure de réclamation, ni de recours ou d'indemnisation, et encore moins de droit disciplinaire.

4. Contrôle et responsabilité

Protéger les droits des citoyens est une chose (en appelant les intéressés à être proactifs et à prendre eux-mêmes des initiatives), une autre est la manière dont le contrôle et la responsabilité sont organisés. Sur ce plan également, la Finlande a prévu des dispositions uniques, en vertu desquelles l'autorité finlandaise de protection des données exerce chaque année des contrôles sur l'administration fiscale finlandaise.

En 2022, cette autorité a estimé que l'administration fiscale finlandaise respectait les exigences du RGPD en matière de proportionnalité, de finalité et de délais de conservation, et que les systèmes de logging garantissaient la responsabilité individuelle des fonctionnaires.

Le ministre peut-il indiquer si l'APD exerce des contrôles de cette nature vis-à-vis du fisc en Belgique? Ceux-ci sont-ils comparables à ce qui existe en Finlande? Quelles sont les conclusions qui en découlent? Une remédiation est-elle nécessaire?

Certes, le système finlandais ne fonctionne pas non plus parfaitement. Ainsi, il a été recommandé d'envoyer plus rapidement la notification aux citoyens et d'intensifier les formations internes sur la minimisation des données. En Belgique, les notifications sont en tout cas inexistantes, sauf si la personne concernée en fait la demande. Le ministre peut-il préciser si des formations internes sur la minimisation de données sont organisées au SPF Finances en rapport avec le PCC (et si elles le seront à l'avenir en ce qui concerne *money control*)?

Une deuxième forme de contrôle est exercée sur l'équivalent finlandais du PCC par deux commissions du Parlement finlandais compétentes en matière de contrôle de la constitutionnalité et de contrôle budgétaire.

Zij evalueren de efficiëntie en de integriteit van het Finse systeem. Jaarlijks wordt het integriteitsverslag van de Finse belastingdienst besproken in een openbare zitting en wordt de minister van Financiën gehoord over de naleving van privacynormen. Dit lijkt de spreker een na te volgen voorbeeld.

Ten slotte controleert de Finse Rekenkamer, tegenhanger van het Belgische Rekenhof, ook de rechtmatigheid van uitgaven door middel van een onafhankelijke audit.

Het zou interessant zijn om tevens een advies te vragen van het Rekenhof over *“money control”*. Het Rekenhof kan immers nagaan of digitale efficiëntie gecombineerd wordt met robuuste, rechtsstatelijke waarborgen.

— België: een cultuur van wantrouwen

Een groot verschil tussen België en Finland is dat het vermoeden van onschuld wordt omgedraaid: de burger moet bewijzen dat hij onschuldig is. Vertrouwen wordt vervangen door wantrouwen; alle Belgen worden als potentiële fraudeurs beschouwd. Door het instellen van *“money control”* creëert de minister een kadaster van wantrouwen.

Een onbetrouwbare overheid leidt tot op zijn beurt tot wantrouwen in de samenleving. Het is logisch dat meer mensen er in een dergelijk klimaat de kantjes van af lopen, in tegenstelling tot de cultuur van vertrouwen waarop Zweden en Finland steunen.

Het betalen van belastingen maakt in Finland of Zweden deel uit van een sociaal contract. Dit houdt onder meer in dat de belastingdienst actief en transparant communiceert en dat burgers weten over welke gegevens de overheid al dan niet beschikt en wat er mee gebeurt.

Ook Belgische burgers beginnen zich dankzij onderhavig debat af te vragen wat er met hun gegevens aan het gebeuren is. Het CAP en *“money control”* genoten tot voor kort zeer weinig bekendheid, maar ondertussen komen er signalen van verzet. Dit doorkruist de socialistische plannen om deze wetgeving snel en zonder veel ruchtbaarheid door het Parlement te loodsen. De heer Van Quickenborne verwijst naar het succesvolle verzet tegen *chat control*, dat in België onder meer werd gevoerd door de heer Kjell Vander Elst (Open Vld) in de Kamer. De heer Vander Elst is klaar voor eenzelfde strijd tegen *“money control”*, door bijvoorbeeld op sociale media te mobiliseren tegen deze aanslag op de privacy van de burgers. Leden van een liberale fractie

Ces commissions évaluent l'efficacité et l'intégrité du système finlandais. Chaque année, le rapport d'intégrité de l'administration fiscale finlandaise est débattu en séance publique et le ministre des Finances est entendu sur le respect des normes de protection de la vie privée. L'intervenant considère qu'il s'agit là d'un exemple à suivre.

Enfin, la Cour des comptes finlandaise, qui constitue l'équivalent de la Cour des comptes belge, contrôle également la légalité des dépenses au moyen d'un audit indépendant.

Il serait intéressant de solliciter également l'avis de la Cour des comptes au sujet de *money control*. La Cour des comptes pourrait en effet vérifier si celui-ci combine efficacité numérique et garanties solides inhérentes à l'état de droit.

— La Belgique: une culture de la méfiance

Une différence majeure entre la Belgique et la Finlande sera le renversement de la présomption d'innocence: il incombera désormais au citoyen belge de prouver son innocence. La confiance sera remplacée par la méfiance et tous les Belges seront considérés comme des fraudeurs potentiels. En instaurant *money control*, le ministre créera un cadastre de la méfiance.

Des pouvoirs publics peu fiables suscitent à leur tour de la méfiance au sein de la société. Dans ce climat, il est logique que davantage de contribuables cherchent des échappatoires. Cela va à rebours de la culture de la confiance qui règne en Suède et en Finlande.

En Finlande ou en Suède, le paiement des impôts s'inscrit dans le cadre d'un contrat social, qui implique notamment que l'administration fiscale communique de manière active et transparente et que les citoyens soient informés des données qui sont à la disposition des pouvoirs publics, ainsi que du traitement de celles-ci.

Grâce au débat actuel, les citoyens belges commencent eux aussi à se demander quel est le traitement réservé à leurs données. Jusqu'il y a peu, le PCC et *money control* étaient très peu connus, mais on observe désormais des signes d'opposition. Cette opposition contrecarre les plans socialistes visant à faire adopter cette législation rapidement et sans trop de bruits au Parlement. M. Van Quickenborne évoque l'opposition victorieuse contre *chat control*, qui, en Belgique, a notamment été menée par M. Kjell Vander Elst (Open Vld) à la Chambre. M. Vander Elst est prêt à mener le même combat contre *money control*, par exemple en mobilisant les réseaux sociaux contre cette atteinte à la vie privée des citoyens. Les membres d'un groupe

kunnen immers niet aanvaarden dat het vermoeden van onschuld wordt omgedraaid.

De minister zal hiermee het vertrouwen in de overheid nog verder doen kelderen (zoals dat reeds het geval is voor de huidige regering). In Nederland is dit vertrouwen na de toeslagenaffaire bijvoorbeeld gedaald naar 4 %. De kost voor de maatschappij bedroeg meer dan 10 miljard euro, meer dan duizend kinderen werden uit hun huis zijn gezet en tienduizenden mensen moesten plotseling onterecht geheven belastingen betalen.

Indien de minister het Nederlandse voorbeeld wenst te volgen, dan zet hij best door met “*money control*”. Volgt hij het Scandinavische voorbeeld, dan past hij het systeem aan. Volgens de *European Social Survey* van 2022 vertrouwt 84 % van de Finnen hun belastingdienst, een cijfer waar de Belgische fiscus en andere overheidsinstanties alleen maar van kunnen dromen. Door plannen zoals het voorliggende wetsontwerp draagt de minister bij tot het wantrouwen van mensen in de fiscus. In een klimaat van vertrouwen zou er geen behoefte zijn aan een dergelijke intrusieve surveillance.

— *Verschillen tussen het Finse en Belgische model: synthese*

De eerste reden waarom het Finse model veel sterker is dan het Belgische is te zoeken in deze cultuur van vertrouwen.

Tekenend is dat de minister van Justitie, mevrouw Annelies Verlinden, bijvoorbeeld nog steeds voorstander is van *chat control*. Daarbovenop zal de minister van Financiën en Pensioenen door middel van “*money control*” ook de geldstromen van burgers controleren. Eenzelfde patroon is zichtbaar bij de plannen voor een databank voor de controle op artsen en hun voorschriften. De spreker gewaagt van een controlelawine.

N-VA beweert soms dat het liberale gedachtegoed te verdedigen. Dat is volgens de heer Van Quickenborne volstrekt ongeloofwaardig: met de voorliggende maatregel wordt bewezen dat de minister zich niets aantrekt van de privacy.

Ten tweede is naast de cultuur van vertrouwen ook een cultuur van digitale veiligheid en cyberbescherming aantoonbaar. De Finse overheid investeert zwaar in gegevensbeveiliging. Alle fiscale data worden opgeslagen in een nationale overheidscloud met redundante service in Finland zelf. Kan de minister toelichten hoe dat in België zit? Wat indien de datawarehouse, waarin ruim driehonderd miljoen gegevens zullen worden opgeslagen,

libéral ne peuvent en effet pas accepter le renversement de la présomption d’innocence.

Avec son projet, le ministre ne fera qu’affaiblir encore davantage la confiance dans les pouvoirs publics (une situation que connaît déjà le gouvernement actuel). Aux Pays-Bas, par exemple, cette confiance a chuté à 4 % après l’affaire des allocations familiales. Le coût de ce scandale pour la société se chiffrait à plus de 10 milliards d’euros, plus d’un millier d’enfants ont été expulsés de leur domicile et des dizaines de milliers de personnes ont dû soudainement payer des impôts indûment prélevés.

Si le ministre souhaite suivre l’exemple néerlandais, il lui suffit de poursuivre la mise en œuvre de *money control*. S’il souhaite en revanche suivre l’exemple scandinave, il devra modifier son système. Selon l’Enquête sociale européenne de 2022, 84 % des Finlandais font confiance à l’administration fiscale, un chiffre dont ne peuvent que rêver l’administration fiscale belge et les autres autorités publiques. En déposant des projets tels que le projet de loi à l’examen, le ministre contribue à la méfiance des citoyens à l’égard de l’administration fiscale. Dans un climat de confiance, un contrôle aussi intrusif ne serait pas nécessaire.

— *Différences entre les modèles finlandais et belge: synthèse*

La première raison pour laquelle le modèle finlandais est nettement plus efficace que le modèle belge réside dans cette culture de confiance.

Il est frappant que Mme Annelies Verlinden, ministre de la Justice, demeure par exemple favorable à *chat control*. De surcroît, *money control* permettra au ministre des Finances et des Pensions de contrôler également les flux financiers des citoyens. La même logique sous-tend les projets de création d’une banque de données en vue de contrôler les médecins et leurs prescriptions. L’intervenant évoque une avalanche de contrôles.

La N-VA affirme parfois qu’elle défend l’idéologie libérale. Selon M. Van Quickenborne, cette affirmation manque totalement de crédibilité: la mesure proposée prouve que le ministre ne se soucie guère du respect de la vie privée.

Deuxièmement, outre la culture de la confiance, il existe aussi en Finlande une culture de la sécurité numérique et de la cyberprotection. Les pouvoirs publics finlandais investissent massivement dans la sécurité des données. Toutes les données fiscales sont conservées dans une infrastructure en ligne (*cloud*) des autorités nationales qui est répliquée en Finlande même. Le ministre peut-il expliquer comment cela se passe en Belgique? Que se

plotseling lekken vertoont? De potentiële gevolgen zijn zeer groot wanneer bankrekeningnummers, saldi en identiteiten openbaar zouden worden.

Indien men niet kan verzekeren dat het systeem cyberveilig is, lijkt het te gevaarlijk. In Finland valt cyberbeveiliging overigens onder het National Cyber Security Center, dat rapporteert aan het ministerie van Transport en Communicatie.

In België bestaat nauwelijks een gelijkaardige cultuur en is er permanent sprake van inbreuken, aanvallen en hacks. Een potentieel lek vanuit Rusland zou bijvoorbeeld mogelijkheden kunnen openen om de rekeningen van 11 miljoen Belgen te plunderen, met een ernstige verarming tot gevolg. De minister neemt een zeer groot risico.

Een derde verschil tussen Finland en België is dat de Grondwetscommissie van het Finse Parlement wetsontwerpen aanpast en afwijst als er een risico bestaat voor de privacy. Zo moest in 2020 bijvoorbeeld het Nationaal Dataplatform hertekend worden omdat deze Grondwetscommissie geoordeeld had dat de algemene koppeling van administratieve databanken niet te verzoenen is met de Finse Grondwet en de beginstelen van doelbinding.

In de Kamer bleek het echter niet mogelijk om een advies te bekomen van de commissie voor Grondwet en Institutionele Hervorming, die nochtans met kennis van zaken kan oordelen. De spreker roept op om hen dit vraagstuk alsnog voor te leggen. Aangezien er deze regeerperiode geen staats Hervorming meer komt, heeft die commissie minder activiteiten en kan zij zich met dergelijke vraagstukken bezighouden.

Een *Data Protection Impact Assessment* (DPIA), waartoe de Raad van State adviseerde alvorens de bespreking van dit wetsontwerp aan te vatten, kwam er trouwens evenmin. Beschermingsmechanismen voor de burger blijven achterwege.

De heer Van Quickenborne stelt dat Finland met zijn cultuur van vertrouwen, veiligheid en grondrechten een voorbeeld vormt waaraan België zich zou moeten spiegelen. De vergelijking tussen beide landen is kristalhelder.

passerait-il si l'entrepôt de données, qui hébergera plus de trois cents millions de données, était subitement en proie à des fuites? Les conséquences potentielles d'une publication des numéros de compte bancaire, des soldes et des identités des titulaires de ces comptes seraient très importantes.

Si l'on ne peut pas garantir que le système sera sécurisé sur le plan informatique, ce stockage de données semble trop dangereux. En Finlande, la cybersécurité relève d'ailleurs du Centre national finlandais de cybersécurité (National Cyber Security Center), qui fait rapport au ministère des Transports et des Communications.

En Belgique, une culture similaire est pratiquement inexistante, et les violations, attaques et piratages sont permanents. Une fuite potentielle orchestrée par la Russie pourrait par exemple ouvrir la voie au pillage des comptes des 11 millions de Belges, ce qui entraînerait un grave appauvrissement. Avec son projet, le ministre prend un risque considérable.

Troisième différence entre la Finlande et la Belgique: la commission de la Constitution du Parlement finlandais modifie et rejette les projets de loi s'ils présentent un risque pour le respect de la vie privée. Par exemple, en 2020, la plate-forme nationale finlandaise de données a dû être remodelée parce que cette commission avait estimé que l'interconnexion généralisée des banques de données administratives était contraire à la Constitution finlandaise et aux principes de la limitation des finalités.

À la Chambre, il est toutefois apparu qu'il n'était pas possible d'obtenir l'avis de la commission de la Constitution et du Renouveau institutionnel, qui pourrait pourtant se prononcer en connaissance de cause. L'intervenant demande que cette question lui soit tout de même soumise. Dès lors qu'aucune réforme de l'État ne sera plus menée sous la présente législature, la charge de travail de cette commission sera réduite et celle-ci pourrait examiner des questions de ce type.

Une analyse d'impact relative à la protection des données (AIPD), que le Conseil d'État a recommandé de réaliser avant d'entamer les discussions sur le projet de loi à l'examen, n'a d'ailleurs pas non plus été effectuée. Les mécanismes de protection en faveur des citoyens font défaut.

M. Van Quickenborne indique que, forte de sa culture de la confiance, de la sécurité et de la protection des droits fondamentaux, la Finlande est un exemple dont la Belgique devrait s'inspirer. La comparaison entre les deux pays est limpide.

Zo worden in Finland de financiële gegevens beheerd door de banken zelf, terwijl in België het Centraal Aanspreekpunt (CAP) deze taak vervult. Dat leidt tot een gedecentraliseerd systeem in Finland en een gecentraliseerd systeem in België.

De toegang tot gegevens gebeurt in Finland uitsluitend door de bevoegde minister, en enkel in het kader van een concreet dossier met motivering. In België bestaat een automatische en permanente toegang. Profileren en datamining zijn in Finland verboden, maar zullen in België worden toegelaten ingevolge de ingediende amendementen.

De kennisgeving aan burgers is in Finland verplicht, terwijl in België burgers, bij ontstentenis aan een regeling, burgers zelf hun gegevens moeten opvragen. Vorig jaar vroegen vier burgers informatie op bij het CAP, terwijl er meer dan 300.000 bevestigingen plaatsvonden.

Het toezicht wordt in Finland bewaakt door een onafhankelijke gegevensbeschermingsautoriteit en het Parlement. In België bestaat er geen regeling, al heeft de Gegevensbeschermingsautoriteit wel een advies uitgebracht.

In Finland is bij elke stap een menselijke tussenkomst vereist. In het onderhavige wetsontwerp en de amendementen wordt dit aspect onvoldoende uitgewerkt, hoewel het noodzakelijk zou zijn om te bepalen hoe de belastingadministratie moet omgaan met vragen van burgers over dossiers waarin een mogelijke onregelmatigheid via datamining naar boven is gekomen.

Vervolgens benadrukt de spreker het belang dat in Finland wordt toegekend aan een cultuur van vertrouwen, proportionaliteit en transparantie, die in schril contrast staat met de cultuur van controle, surveillance en toezicht in België. Op dit stuk scoren alle genoemde voorbeelden (Duitsland, Oostenrijk, Nederland, Zweden en Finland) beter dan België. Toch kiest de minister voor meer staatscontrole. Dit doet hij volgens de spreker in navolging van de socialistische regeringspartner, die ook in de Vlaamse regering blij zou geven van minachting voor de privacy en burgers wantrouwt in plaats van hen te ondersteunen. Het gevolg van deze keuzes is volgens de heer Van Quickenborne een verdere toename van overheidsuitgaven en de creatie van bijkomende controlemechanismen, wat leidt tot bijkomende administratieve functies die niet bijdragen aan de economische noden van het land.

In Finland staat subsidiariteit centraal. De heer Van Quickenborne herinnert eraan dat de minister zich

Tandis qu'en Finlande, les données financières sont gérées par les banques elles-mêmes, en Belgique, c'est le Point de contact central (PCC) qui se charge de cette mission. Le système finlandais est donc décentralisé tandis que le système belge est centralisé.

En Finlande, seul le ministre compétent peut accéder aux données et uniquement dans le cadre d'un dossier concret et d'une demande motivée. En Belgique, l'accès est automatique et permanent. Le profilage et le *data mining* sont interdits en Finlande, mais ils seront autorisés en Belgique si les amendements présentés sont adoptés.

La notification aux citoyens est obligatoire en Finlande, tandis qu'en Belgique, faute de réglementation, les citoyens doivent eux-mêmes demander leurs données. L'année dernière, quatre citoyens ont demandé des informations au PCC, alors que plus de 300.000 consultations de données ont eu lieu.

Dans le système finlandais, le contrôle des procédures est assuré par une autorité de protection des données indépendante et par le Parlement. En Belgique, il n'existe aucune réglementation, bien que l'Autorité de protection des données ait émis un avis.

La Finlande impose une intervention humaine à chaque étape du processus. Dans le projet de loi et dans les amendements à l'examen, cette question n'est pas suffisamment traitée. Pourtant, il serait nécessaire de déterminer comment l'administration fiscale doit traiter les questions des citoyens concernant les dossiers dans lesquels une irrégularité potentielle a été mise en évidence par la voie du *data mining*.

L'intervenant souligne ensuite l'importance accordée en Finlande à une culture de confiance, de proportionnalité et de transparence, culture qui contraste nettement avec la culture de contrôle, de surveillance et de supervision en Belgique. Sur ce point, tous les pays cités (Allemagne, Autriche, Pays-Bas, Suède et Finlande) font mieux que la Belgique. Pourtant, le ministre opte pour davantage de contrôle par l'État. L'intervenant y perçoit l'influence du partenaire socialiste du gouvernement, qui, selon lui, ferait également preuve de mépris pour la vie privée au sein du gouvernement flamand et se méfierait des citoyens au lieu de les soutenir. D'après M. Van Quickenborne, ces choix entraîneront une nouvelle augmentation des dépenses publiques et la création de mécanismes de contrôle supplémentaires, ce qui entraînera la création de nouvelles fonctions administratives qui ne répondront en rien aux besoins économiques du pays.

En Finlande, la subsidiarité est centrale. M. Van Quickenborne rappelle que, par le passé, le

in het verleden voor subsidiariteit uitsprak, onder meer in het kader van staatshervormingen. Met het voorliggende wetsontwerp gaat men echter in de richting van een centralistisch systeem dat burgers wantrouwt en waarin subsidiariteit wordt genegeerd.

De Raad van State verzoekt om een gegevensbeschermingseffectbeoordeling. In Finland wordt zo een beoordeling systematisch uitgevoerd. Daarbij onderzoekt men steeds of het doel met minder persoonsgegevens kan worden bereikt en of minder ingrijpende middelen mogelijk zijn. Pas wanneer het antwoord ontkennend is, mag een verwerking plaatsvinden.

De spreker benadrukt dat fiscale efficiëntie niet ten koste mag gaan van de grondrechten en dat zijn partij als enige die grondrechten principieel verdedigt. Het thema krijgt in toenemende mate maatschappelijke aandacht. De spreker verwijst naar een artikel in de pers waarin burgers hun bezorgdheid uiten over de door de Franse president voorgestelde afzwakking van Europese privacyregels in het kader van fiscale controles. Zo dreigt Europa richting een systeem te evolueren waarin zowel overheden als private ondernemingen systematisch persoonsgegevens controleren. De voorgestelde wijziging van artikel 22 van de AVG is onaanvaardbaar. Dat artikel vormt tevens de juridische basis voor *money control*, aangezien de Raad van State en de Gegevensbeschermingsautoriteit in hun adviezen expliciet naar dat artikel verwijzen.

De spreker benadrukt dat Finland, dat sterk inzet op vertrouwen in burgers, een inningsgraad van meer dan 91 % en een nalevingsgraad van 97 % bereikt. De fiscale kloof bedraagt er minder dan 1 % van het bruto binnenlands product, terwijl die in België 4 à 5 % bedraagt. Finland toont dan ook aan dat een ondernemersvriendelijk land met een slanke overheid de belastingen efficiënt kan innen met respect voor de privacy van burgers.

De heer Van Quickenborne overloopt de lessen die België kan trekken uit het Finse voorbeeld. Zo zou elke verwerking beperkt moeten blijven tot fiscale doeleinden. Daarnaast moet een verplichte kennisgeving aan burgers worden ingevoerd, naar het voorbeeld van onder meer Hasselt, Bertem en Lochristi, zodat burgers proactief worden geïnformeerd. De GBA moet worden versterkt met een daadwerkelijke sanctiebevoegdheid, opdat negatieve adviezen niet langer zonder gevolg blijven. De centralisatie van gegevens moet worden vermeden om de concentratie van risico's te beperken. Banken moeten daarentegen zelf hun eigen gegevens blijven beheren. Digitalisering moet worden ingezet voor dienstverlening

ministre s'est déjà déclaré favorable au principe de subsidiarité, notamment dans le cadre de réformes de l'État. Cependant, le projet de loi à l'examen va dans le sens d'un système centralisé qui se méfie des citoyens et qui nie ce principe de subsidiarité.

Le Conseil d'État demande une évaluation des effets en matière de protection des données. En Finlande, cette évaluation est systématique. Elle permet de déterminer si l'objectif visé peut être atteint avec moins de données à caractère personnel et s'il existe des moyens moins intrusifs. Ce n'est que lorsque la réponse est négative que le traitement peut avoir lieu.

L'intervenant souligne que la recherche de l'efficacité fiscale ne peut pas justifier d'entamer les droits fondamentaux et que son parti est le seul à défendre ces droits fondamentaux par principe. Ce thème suscite un intérêt croissant dans la société. L'intervenant renvoie à un article de presse dans lequel des citoyens expriment leur inquiétude face à l'assouplissement de la portée des règles européennes de protection de la vie privée proposé par le président français dans le cadre des contrôles fiscaux. Ainsi, l'Europe risque d'évoluer vers un système de contrôle systématique des données à caractère personnel par les autorités publiques et les entreprises privées. La modification proposée de l'article 22 du RGPD est inacceptable. Cet article constituera également la base juridique du *money control* puisque le Conseil d'État et l'Autorité de protection des données renvoient explicitement à cet article dans leurs avis respectifs.

L'intervenant souligne que la Finlande, qui mise beaucoup sur la confiance de l'État envers les citoyens, atteint un taux de perception de plus de 91 % et un taux de conformité de 97 %. L'écart fiscal y est inférieur à 1 % du produit intérieur brut alors qu'il est de 4 à 5 % en Belgique. La Finlande démontre donc qu'un pays bienveillant envers les entrepreneurs et doté de pouvoirs publics légers est à même de percevoir efficacement les impôts dans le respect de la vie privée des citoyens.

M. Van Quickenborne passe en revue les enseignements que la Belgique peut tirer de l'exemple finlandais. Tout traitement devrait ainsi être limité à des finalités fiscales. De plus, une notification obligatoire aux citoyens devrait être instaurée, à l'instar de ce qui se fait notamment à Hasselt, Bertem et Lochristi, afin que les citoyens soient informés de manière proactive. L'APD devrait être renforcée et dotée d'un véritable pouvoir de sanction, pour que les avis négatifs ne restent plus sans suite. La centralisation des données doit être évitée pour limiter la concentration des risques, tandis que les banques doivent continuer à gérer elles-mêmes leurs propres données. La numérisation doit être mise au service

aan burgers, niet voor toezicht. Tot slot pleit de spreker voor de invoering van een jaarlijks parlementair integriteitsrapport om de transparantie te bevorderen.

Het Finse model van fiscale gegevensverwerking toont aan dat respect voor de grondwet en efficiëntie geen tegenstelling vormen. Vertrouwen leidt net tot meer efficiëntie. In dit kader verwijst de spreker naar een recent doctoraatsonderzoek aan de Universiteit Antwerpen, getiteld *Deus Tax Machina*, waarin wordt gesteld dat een belastingstelsel dat vertrouwen creëert, dat dubbel en dik terugverdient. De spreker meent dat eenvoud, transparantie en vertrouwen de fundamenteën van een modern belastingstelsel vormen, en betreurt dat het voorliggende wetsontwerp net in de tegenovergestelde richting gaat.

De spreker trekt vervolgens een eerste voorlopige conclusie uit de vijf internationale modellen die hij heeft beschreven. Duitsland, Oostenrijk, Nederland, Zweden en Finland hanteren elk een eigen bestuurscultuur, maar delen een essentieel uitgangspunt: de toegang van de overheid tot financiële gegevens is geen recht, maar een uitzonderingsbevoegdheid. Er bestaan duidelijke grenzen aan het gebruik van fiscale en in het bijzonder bancaire gegevens, die zijn opgenomen in wetten met beperkte draagwijdte, en die in contrast staan met de voorliggende amendementen, die een onbeperkte en generieke toegang toestaan. Ook de noodzakelijkheid wordt strikt toegepast: toegang is slechts mogelijk in individuele dossiers, bij concrete vermoedens van belastingontduiking en voor individuele verwerkingen. Overeenkomstig het proportionaliteitsbeginsel wordt bovendien bepaald dat de inmenging in de privacy niet verder mag gaan dan strikt noodzakelijk.

Het fundamentele verschil is niet te wijten aan technologie, aangezien ook België over de nodige technische capaciteit beschikt. Het verschil schuilt in de houding tegenover macht en informatie. De vijf vermelde landen vertrekken van het primaat van het recht, van transparantie en vertrouwen. België kiest voor een logica van administratieve efficiëntie, waarbij rechtswaarborgen ondergeschikt worden gemaakt.

De heer Van Quickenborne stelt dat de registers van de verschillende vermelde landen vergelijkbare structurele kenmerken vertonen. In Duitsland gaat het over het *Kontenregister*, dat sinds 2003 wordt beheerd door de BaFin, de Duitse toezichthouder voor de financiële markten. De toegang is uitsluitend reactief en dossiergebonden: fiscus en de politie mogen enkel zoeken naar rekeningen van een specifiek persoon en uitsluitend na schriftelijke motivering. Het Duitse grondwettelijk hof

des citoyens, et non utilisée comme un instrument de contrôle. Enfin, le membre préconise l'introduction d'un rapport parlementaire annuel sur l'intégrité de manière à promouvoir la transparence.

Le modèle finlandais de traitement des données fiscales démontre que le respect de la Constitution et l'efficacité ne sont pas incompatibles. La confiance engendre précisément une plus grande efficacité. Dans ce cadre, l'intervenant fait référence à une récente thèse de doctorat à l'Université d'Anvers, intitulée *Deus Tax Machina*, qui montre qu'un système fiscal qui inspire confiance se révèle doublement rentable. Le membre estime que la simplicité, la transparence et la confiance constituent les fondements d'un système fiscal moderne, et déplore que le projet de loi à l'examen aille exactement dans la direction opposée.

L'intervenant tire ensuite une première conclusion provisoire à partir des cinq modèles internationaux qu'il a décrits. L'Allemagne, l'Autriche, les Pays-Bas, la Suède et la Finlande possèdent chacun leur propre culture administrative, mais partagent un principe essentiel: l'accès des pouvoirs publics aux données financières n'est pas un droit, mais un pouvoir dérogatoire. Des limites claires encadrent l'utilisation des données fiscales et, en particulier, bancaires. Elles figurent dans des lois à portée limitée, ce qui contraste avec les amendements proposés, qui permettraient un accès illimité et générique. Par ailleurs, le principe de nécessité est strictement appliqué: l'accès n'est autorisé que dans le cadre de dossiers individuels, sur la base de soupçons concrets de fraude fiscale et pour des traitements individuels. Conformément au principe de proportionnalité, il est en outre indiqué que l'ingérence dans la vie privée ne peut pas excéder ce qui est strictement nécessaire.

La différence fondamentale ne réside pas dans la technologie, puisque la Belgique dispose également des capacités techniques nécessaires. Elle tient plutôt à l'attitude adoptée vis-à-vis du pouvoir et de l'information. Les cinq pays mentionnés s'appuient sur la primauté du droit, de la transparence et de la confiance. La Belgique, en revanche, opte pour une logique d'efficacité administrative, dans laquelle les garanties juridiques sont secondaires.

M. Van Quickenborne souligne que les registres des différents pays mentionnés présentent des caractéristiques structurelles similaires. En Allemagne, il s'agit du *Kontenregister*, géré depuis 2003 par la BaFin, l'Autorité fédérale de supervision financière. L'accès est exclusivement réactif et lié à un dossier individuel: le fisc et la police ne peuvent consulter les comptes que d'une personne spécifique et uniquement après avoir fourni une justification écrite. La Cour constitutionnelle

bevestigde in 2022 dat het systeem enkel grondwettig is wanneer profilering en massaal datagebruik worden uitgesloten, terwijl het voorliggende wetsontwerp die praktijken net mogelijk maakt. Deze juridische grenzen steunen op Europese regels en zijn dus ook voor België relevant. De Duitse architectuur kent weliswaar centralisatie, maar ook een juridisch kader, dat in België ontbreekt.

In Oostenrijk werd in 2015 het Oostenrijkse *Kontenregister* ingevoerd. De toegang is er beperkt tot specifieke doeleinden zoals fiscale fraude, witwassen en terrorismefinanciering, en is enkel mogelijk na voorafgaande rechterlijke toestemming. De gegevens blijven gedecentraliseerd bij de banken en bevat het register zelf enkel meta-informatie. Dat leidt tot transparantie van toezicht en geslotenheid van inhoud. Opvragingen worden gelogd en burgers kunnen achteraf nagaan of hun gegevens werden geraadpleegd.

Nederland vormt een bijzonder geval, aangezien de toeslagenaffaire heeft aangetoond dat het land geen modelland is. Toch kunnen uit het Nederlandse model belangrijke lessen worden getrokken, onder meer op grond van het SyRi-arrest van 2020. Dat arrest heeft een systeem van massale datakoppelingen lamgelegd nog vóór de inwerkingtreding. Het Nederlandse systeem blijft digitaal performant maar is juridisch ingeperkt.

Zweden hanteert een model van radicale openbaarheid, waarbij informatie over inkomens en onroerend goed publiek toegankelijk is. De gegevensbeveiliging blijft echter strikt, en de *Skatteverket* beschikt niet over rechtstreekse toegang tot bankrekeningen, maar ontvangt enkel rapporten over rentes en dividenden. Automatische selectie, datamining en profilering zijn in Zweden verboden en de Zweedse gegevensbeschermingsautoriteit ziet er nauwlettend op toe dat proportionaliteit van elke verwerking wordt gewaarborgd.

Tot slot merkt de spreker op dat, indien een keuze gemaakt moet worden, Finland het meest aangewezen model vormt.

Het verschil tussen de vijf onderzochte landen en België is aanzienlijk, aangezien ons land evolueert van controle naar een systeem van massatoezicht, met een CAP dat toegang biedt tot alle bankrekeningen van natuurlijke en rechtspersonen. Hoewel het systeem, dat ingevoerd werd in naleving van Europese verplichtingen, oorspronkelijk gerechtvaardigd was om fraude efficiënt te bestrijden en willekeur tussen banken te vermijden. Aangezien voordien bij vermoedens van fraude alle banken bevraagd moesten worden, kon dat voor bepaalde banken aanleiding geven om, met toepassing van de

allemande a confirmé en 2022 que ce système n'était constitutionnel que si le profilage et l'usage massif des données étaient exclus, alors que le projet de loi à l'examen permet justement ces pratiques. Ces limites juridiques, basées sur les règles européennes, sont également pertinentes pour la Belgique. L'architecture allemande est certes centralisée, mais aussi encadrée juridiquement, ce qui manque en Belgique.

Le *Kontenregister* autrichien, introduit en 2015, n'est accessible que pour des finalités spécifiques telles que la fraude fiscale, le blanchiment et le financement du terrorisme, et uniquement sur autorisation judiciaire préalable. Les données restent décentralisées dans les banques et le registre lui-même ne contient que des méta-informations. Ce dispositif assure la transparence de la surveillance et la confidentialité du contenu. Les consultations sont enregistrées et les citoyens peuvent vérifier *a posteriori* si leurs données ont été consultées.

Les Pays-Bas constituent un cas particulier: l'affaire des allocations familiales a montré que le pays n'était pas exemplaire. Le modèle néerlandais permet toutefois de tirer des enseignements importants, notamment avec l'arrêt SyRi de 2020, qui a paralysé un système de couplage massif de données avant même son entrée en vigueur. Bien que le système soit performant sur le plan numérique, il reste encadré sur le plan juridique.

La Suède suit un modèle de transparence radicale, dans lequel les informations sur les revenus et les biens immobiliers sont accessibles au public. La sécurité des données reste toutefois strictement garantie, et l'administration fiscale (*Skatteverket*) n'a pas directement accès aux comptes bancaires, mais reçoit uniquement des rapports sur les intérêts et les dividendes. La sélection automatique, le *data mining* et le profilage sont interdits en Suède, et l'autorité suédoise chargée de la protection des données veille de près à ce que la proportionnalité de chaque traitement soit garantie.

Pour conclure, l'intervenant fait observer que, si un choix devait être fait, le modèle finlandais serait le plus approprié.

Il y a une différence considérable entre les cinq pays analysés et la Belgique, dès lors que notre pays passe d'un mécanisme de contrôle à un système de surveillance de masse, avec un PCC qui donne accès à tous les comptes bancaires des personnes physiques et morales. Ce système, qui a été introduit dans le respect des obligations européennes, a pourtant été justifié initialement comme étant une manière de lutter efficacement contre la fraude et d'éviter l'arbitraire entre les banques. Auparavant, en cas de soupçon de fraude, il fallait interroger toutes les banques, ce qui pouvait

know your customer-regels, bankrelaties met de klant in kwestie te verbreken. Met het CAP hoefden enkel de noodzakelijke banken bevestigd te worden. Indien het instrument echter wordt uitgebreid tot een volledig geautomatiseerde data-analyse van alle bankrekeningen en saldi, zal dat leiden tot centrale datamining van de financiële gedragingen van de gehele bevolking. Het is bovendien onduidelijk welk gedrag als afwijkend wordt beschouwd, waardoor misbruik van dit systeem niet kan worden uitgesloten.

De heer Van Quickenborne stelt dat de voorgestelde uitbreiding van het CAP in de vijf voormelde landen niet ingevoerd zou kunnen worden zonder grondwetwijziging, aangezien er in dit kader geen wettelijke noodzaak bestaat voor algemene dataverzameling, massale profilering disproportioneel is, een individueel doel ontbreekt, automatische profilering zonder menselijke toetsing strijdig is met de grondwet, burgers niet geïnformeerd worden en de fiscus beheer, analyse en toezicht cumuleert, wat een machtsonevenwicht creëert. Daarenboven wordt in voldoende Europese rechtsspraak gesteld dat de voorgestelde uitbreiding leidt tot algemene gegevensanalyse, die strijdig is met het EU-recht.

De Belgische regering stelt dat *money control* nodig is voor de bestrijding van fiscale fraude, omdat meer data zal leiden tot meer fiscale rechtvaardigheid. Uit de internationale vergelijking blijkt echter het tegendeel: in landen zonder *money control* wordt meer dan 99 % van de belastingen geïnd, zonder centrale transactiedatabank en zonder massale datamining. De invoering van *money control* zou enkel leiden tot een grotere belastingkloof, een lagere inning van de belastingen en een verminderde bereidheid tot belastingbetaling. De spreker herhaalt dat efficiëntie niet afhangt van controle, maar van juridische duidelijkheid en vertrouwen in burgers.

De heer Van Quickenborne meent dat de vergelijking van de vijf onderzochte Europese modellen tot één conclusie leidt: het Belgische *money control* vormt een structurele breuk met de traditie van de Europese rechtsstaat. België, dat vroeger een pionier was op het gebied van rechtsstaatbescherming en internationaal recht, voert nu wetgeving in die deze traditie ondermijnt, ook in fiscale dossiers. Terwijl België zich decennialang heeft ingespannen op het Europese niveau voor de totstandkoming van de AVG, het Europees Verdrag voor de Rechten van de Mens en het Handvest van de grondrechten van de Europese Unie, voert de regering nu wetgeving in waarmee zij internationale normen en instanties aan de kant schuift. Waar privacy in de vijf

entraîner pour certaines d'entre elles, en vertu des règles d'identification du client (*know your customer*), la rupture des relations bancaires avec le client en question. Grâce au PCC, il ne fallait plus interroger que les banques visées. Néanmoins, si l'instrument est étendu à une analyse de données totalement automatisée de l'ensemble des comptes bancaires et des soldes, cela débouchera sur un *data mining* central des comportements financiers de toute la population. En outre, il n'est pas clairement précisé quel comportement est considéré comme déviant, si bien que le risque d'abus du système ne peut être exclu.

M. Van Quickenborne indique que l'extension proposée du PCC ne pourrait avoir lieu dans les cinq pays précités sans modification de la Constitution, puisqu'il n'existe pas, dans ce cadre, de nécessité légale pour une collecte généralisée de données, que le profilage massif est disproportionné, qu'une finalité individuelle fait défaut, que le profilage automatique sans contrôle humain est contraire à la Constitution, que les citoyens ne sont pas informés et que l'administration fiscale cumule gestion, analyse et contrôle, ce qui crée un déséquilibre des pouvoirs. De plus, il existe une jurisprudence européenne abondante, dont il ressort que l'extension proposée entraîne une analyse générale de données qui est contraire au droit européen.

Le gouvernement belge déclare que le *money control* est nécessaire pour lutter contre la fraude fiscale, parce que l'accès à plus de données conduira à plus de justice fiscale. La comparaison internationale prouve pourtant le contraire: des pays qui n'appliquent pas de *money control* perçoivent plus de 99 % des impôts, sans banque de données centrale des transactions ni *data mining* massif. L'instauration du *money control* aurait seulement pour effet de creuser le fossé fiscal, de réduire le taux de perception des impôts et de rendre les contribuables moins enclins à payer leurs impôts. L'intervenant répète que l'efficacité ne dépend pas du contrôle, mais de la clarté juridique et de la confiance envers les citoyens.

M. Van Quickenborne estime que la comparaison des cinq modèles européens analysés débouche sur une seule conclusion: le système belge de *money control* constitue une rupture structurelle avec la tradition de l'État de droit européen. La Belgique, qui était auparavant pionnière dans le domaine de la protection de l'état de droit et du droit international, introduit désormais une législation qui bafoue cette tradition, y compris en matière fiscale. Alors que la Belgique s'est démenée pendant des décennies au niveau européen pour faire adopter le RGPD, la Convention européenne des droits de l'homme, ainsi que la Charte des droits fondamentaux de l'Union européenne, le gouvernement introduit aujourd'hui une législation qui fait fi des normes et des

voormelde landen als een grondwettelijke drempel geldt, wordt het in België als een probleem beschouwd.

Andere landen vertrouwen op menselijke beoordeling, terwijl het Belgische systeem evolueert naar algoritmische preventie. Het CAP bevat alle bankrekeningen van natuurlijke personen in België, met bijbehorende saldi en financiële contracten. Bij een foutenmarge van 1 % zouden 110.000 personen ten onrechte als verdacht kunnen worden aangemerkt. Ondanks dat risico worden algoritmes toch verkozen boven menselijke toetsing.

In de vijf voormelde landen is transparantie de norm, terwijl in België geslotenheid overheerst. *Money control* is een nieuw paradigma waarin iedere burger *a priori* verdacht wordt en de uitzondering de regel wordt. Dat is veel te verregaand.

Naast de vijf voormelde systemen die eerder tot Germaanse of Scandinavische landen behoren, heeft de spreker ook andere internationale modellen onderzocht, onder andere het Angelsaksische model van Ierland, alsook het Luxemburgse en het Zwitserse model.

De heer Van Quickenborne bespreekt ten eerste het Ierse model van een centraal bankrekeningregister, het *Ireland Safe Deposit Box Bank and Payment Accounts Register* (ISBAR). Het register werd ingevoerd bij de in 2021 gewijzigde *Criminal Justice (Money Laundering and Terrorist Financing) Act* van 2010, waarmee uitvoering werd gegeven aan de vierde antiwitwasrichtlijn (2015/849) van de Europese Unie⁹. Het ISBAR wordt beheerd door de Ierse belastingdienst (*Revenue Commissioners*) in samenwerking met het Ierse ministerie van Financiën (*Department of Finance*), onder toezicht van de Ierse gegevensbeschermingsautoriteit (*Data Protection Commission – DPC*). De wettelijke grondslag wordt gevormd door S.I. nr. 233/2020¹⁰, S.I. nr. 321/2021¹¹ en de voormelde *Criminal Justice (Money Laundering and Terrorist Financing) Act*. Het register heeft als doel natuurlijke en rechtspersonen te identificeren die een bank- of betaalrekening in Ierland aanhouden, witwas- en

instances internationales. Alors que le respect de la vie privée représente un pilier constitutionnel dans les cinq pays cités, il est considéré comme un problème en Belgique.

D'autres pays font confiance au jugement humain, tandis que le système belge évolue vers une prévention algorithmique. Le PCC contient tous les comptes bancaires des personnes physiques en Belgique, avec les soldes et les contrats financiers y afférents. Avec une marge d'erreur de 1 %, 110.000 personnes pourraient être considérées, à tort, comme suspectes. En dépit de ce risque, les algorithmes sont préférés au contrôle humain.

Si la transparence est la norme dans les cinq pays cités, c'est l'opacité qui règne en Belgique. Le *money control* constitue un nouveau paradigme, dans lequel chaque citoyen est suspect *a priori* et l'exception devient la règle. Cela va beaucoup trop loin.

Outre les cinq systèmes cités qui correspondent plutôt à des pays germaniques ou scandinaves, l'intervenant a aussi examiné d'autres modèles dans le monde, entre autres le modèle anglo-saxon de l'Irlande, ainsi que les modèles luxembourgeois et suisse.

M. Van Quickenborne aborde tout d'abord le modèle irlandais de registre central des comptes bancaires, l'*Ireland Safe Deposit Box Bank and Payment Accounts Register* (ISBAR). Ce registre a été introduit par la loi de 2010 sur la Justice pénale (blanchiment d'argent et financement du terrorisme) (*Criminal Justice (Money Laundering and Terrorist Financing) Act*), modifiée en 2021, qui transpose la quatrième directive anti-blanchiment (2015/849) de l'Union européenne⁹. L'ISBAR est géré par l'administration fiscale irlandaise (*Revenue Commissioners*) en collaboration avec le ministère irlandais des Finances (*Department of Finance*), sous le contrôle de l'autorité irlandaise de protection des données (*Data Protection Commission – DPC*). La base légale est constituée par le S.I. n° 233/2020¹⁰, le S.I. n° 321/2021¹¹ et la loi précitée (*Criminal Justice (Money Laundering and Terrorist Financing) Act*). Le registre a pour objectif d'identifier les personnes physiques

⁹ Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2005/60/EG van het Europees Parlement en de Raad en Richtlijn 2006/70/EG van de Commissie (Voor de EER relevante tekst)

¹⁰ S.I. No. 233/2020 – European Union (Modifications of Statutory Instrument No. 110 of 2019) (Registration of Beneficial Ownership of Certain Financial Vehicles) Regulations 2020.

¹¹ S.I. No. 321/2021 – European Union (Modifications of Statutory Instrument No. 110 of 2019) (Registration of Beneficial Ownership of Certain Financial Vehicles) (Amendment) Regulations 2021

⁹ Directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission (Texte présentant de l'intérêt pour l'EEE)

¹⁰ S.I. No. 233/2020 – European Union (Modifications of Statutory Instrument No. 110 of 2019) (Registration of Beneficial Ownership of Certain Financial Vehicles) Regulations 2020.

¹¹ S.I. No. 321/2021 – European Union (Modifications of Statutory Instrument No. 110 of 2019) (Registration of Beneficial Ownership of Certain Financial Vehicles) (Amendment) Regulations 2021

fraudeonderzoeken te ondersteunen en internationale samenwerking te faciliteren.

Het ISBAR bevat uitsluitend basisidentificatiegegevens: naam van de rekeninghouder, adres of registratienummer, bank of betalingsinstelling, IBAN, datum van opening en sluiting van de rekening en eventuele gevolmachtigden. Saldi, transactiegegevens en andere financiële waarden worden niet opgenomen. In België worden daarentegen welaldi en financiële waarden geregistreerd.

Het ISBAR telt vijf categorieën van informatiegerechtigden: de belastingdienst voor beheer en raadpleging, de instantie voor de inbeslagname van goederen (het *Criminal Assets Bureau*) voor operationeel gebruik, de financiële inlichtingeneenheid en de politie voor consultatie, en de centrale bank voor toezichtdoeleinden. Elke toegang vereist een dossiernummer, een juridisch mandaat, automatische logging en naleving van de richtlijnen inzake *Data Protection Impact Assessment* (DPIA). In vergelijking hebben in België heel wat meer actoren toegang tot het CAP en wordt er geen DPIA opgesteld.

De heer Lode Vereeck (VB) bevestigt dat er geen documenten beschikbaar zijn waaruit blijkt dat er een DPIA of een regelgevingsimpactanalyse werd opgesteld, terwijl hij meent dat een dergelijke analyse verplicht is.

De heer Vincent Van Quickenborne (Open Vld) merkt op dat in Ierland datamining bij wet verboden is, aangezien artikel 10 van de relevante regelgeving stelt dat geautomatiseerde analyses, datamining of profilering van het ISBAR alleen mogen worden uitgevoerd indien strikt noodzakelijk voor de technische integriteit van het systeem. Enkel gerichte zoekopdrachten per persoon of entiteit zijn toegelaten, bulkquery's en patroonherkenning zijn verboden, en de financiële inlichtingeneenheid en de politie mogen zoekopdrachten uitsluitend binnen concrete onderzoeken uitvoeren.

De DPC licht logbestanden door en ziet erop toe dat geen algoritmische koppeling plaatsvindt tussen het ISBAR en andere databanken, zoals het register van uiteindelijke begunstigen (*Beneficial Ownership Register*), dat inzicht biedt in de achterliggende aandeelhouders. Overigens heeft de spreker positieve geluiden gehoord over de door de minister voorbereide vereenvoudiging van het vergelijkbare Belgische UBO-register.

et morales qui détiennent un compte bancaire ou un compte de paiement en Irlande, de soutenir les enquêtes sur le blanchiment d'argent et la fraude et de faciliter la coopération internationale.

L'ISBAR ne contient que des données d'identification de base: nom du titulaire du compte, adresse ou numéro d'enregistrement, banque ou établissement de paiement, IBAN, date d'ouverture et de clôture du compte et éventuels mandataires. Les soldes, les données relatives aux transactions et autres valeurs financières ne sont pas enregistrés. En Belgique, en revanche, les soldes et les valeurs financières sont bel et bien enregistrés.

L'ISBAR compte cinq catégories de personnes habilitées à recevoir l'information: l'administration fiscale pour la gestion et la consultation, l'autorité chargée de la saisie de biens (le *Criminal Assets Bureau*) pour l'utilisation opérationnelle, la cellule de renseignement financier et la police pour la consultation, et la banque centrale à des fins de surveillance. Chaque accès nécessite un numéro de dossier, un mandat juridique, un logging automatique et le respect des directives relatives à l'Analyse d'impact relative à la protection des données (AIPD). En comparaison, en Belgique, le nombre d'acteurs ayant accès au PCC est beaucoup plus élevé et aucune AIPD n'est effectuée.

M. Lode Vereeck (VB) confirme qu'aucun document attestant la réalisation d'une AIPD ou d'une analyse d'impact de la réglementation n'est disponible, alors qu'il estime qu'une telle analyse est obligatoire.

M. Vincent Van Quickenborne (Open Vld) fait observer qu'en Irlande, le *data mining* est interdit par la loi, puisque l'article 10 de la réglementation applicable prévoit que les analyses automatisées, le *data mining* ou le profilage de l'ISBAR ne peuvent être effectués que s'ils sont strictement nécessaires à l'intégrité technique du système. Seules les recherches ciblées par personne ou par entité sont autorisées, les requêtes en masse et la reconnaissance de modèles sont interdites, et la cellule de renseignement financier et la police ne peuvent effectuer des recherches que dans le cadre d'enquêtes concrètes.

La DPC examine les fichiers de journalisation et veille à ce qu'aucun lien algorithmique ne soit établi entre l'ISBAR et d'autres banques de données, telles que le registre des bénéficiaires effectifs (*Beneficial Ownership Register*), qui fournit des informations sur les actionnaires qui se trouvent derrière les structures. Par ailleurs, l'intervenant a entendu des échos positifs sur la simplification du registre UBO, registre similaire en Belgique, préparée par le ministre.

Technisch gezien rapporteren de banken in Ierland dagelijks op het *Revenue Online Service*-platform (ROS) in een gestandaardiseerde XML-structuur. De gegevens worden versleuteld opgeslagen in de cloud van de Ierse belastingdienst. De bewaartermijn bedraagt vijf jaar na sluiting van de rekening, terwijl dat tien jaar is in België. Toegang vindt plaats via het API-portaal *ISBAR Portal for Authorized Users*. Het systeem registreert ongeveer twaalf miljoen actieve rekeninggegevens, terwijl dat er in België meer dan driehonderd miljoen zijn.

Voor de invoering van het ISBAR heeft de DPC het systeem getoetst aan de AVG. Er werden drie garanties ingevoerd, namelijk de logging van alle query's met real-time meldingen aan de DPC bij afwijkingen, een strikte beperking van toegang tot erkende opsporingsdiensten en een verbod op geautomatiseerde risico-classificatie of scoring. Het systeem werd door de DPC als AVG-conform en proportioneel beoordeeld.

Op internationaal vlak is Ierland aangesloten op het *Bank Account Registers Interconnection System* (BARIS), dat registers van alle EU-lidstaten verbindt. Buitenlandse verzoeken tot toegang moeten handmatig door de Ierse belastingdienst worden goedgekeurd. Er is geen centrale Europese datamining mogelijk; elke lidstaat behoudt eigen toegang en logging.

De heer Van Quickenborne somt de sterktes van het Ierse ISBAR-systeem op: zeer hoge datakwaliteit en snelle responstijden, transparante governance, sterke juridische afbakening van de bevoegdheden en volledige naleving van de Europese antiwitwas-richtlijnen. Het is onduidelijk of het systeem met betrekking tot het CAP dezelfde sterktes zou bezitten.

De zwaktes van het Ierse systeem zijn het ontbreken van een directe koppeling met het UBO-register, het ontbreken van analytische functies en het feit dat het systeem enkel fysiek gehost wordt bij de belastingdienst, zonder gedeelde infrastructuur met de Ierse financiële inlichtingeneenheid.

Wat betreft de publieke perceptie van het ISBAR blijkt uit een peiling dat 78 % van de respondenten de ISBAR-wetgeving als noodzakelijk en evenwichtig beschouwt. De spreker zou van de minister willen vernemen wat de publieke perceptie van het CAP in België is.

D'un point de vue technique, les banques irlandaises transmettent quotidiennement leurs données au travers de la plateforme *Revenue Online Service* (ROS), dans un format XML standardisé. Les données sont stockées de manière cryptée dans le cloud de l'administration fiscale irlandaise. La durée de conservation est de cinq ans après la clôture du compte, alors qu'elle est de dix ans en Belgique. L'accès se fait via le portail API *ISBAR Portal for Authorized Users*. Le système enregistre environ douze millions de données de comptes actifs, contre plus de trois cents millions en Belgique.

Avant la mise en place de l'ISBAR, la DPC a vérifié la conformité du système avec le RGPD. Trois garanties ont été mises en place, à savoir le logging de toutes les requêtes avec signalement en temps réel à la DPC en cas d'anomalies, une restriction stricte de l'accès aux services d'enquête agréés et une interdiction de la classification automatisée des risques ou de l'utilisation automatique de scores de risque. La DPC a jugé que le système était conforme au RGPD et proportionné.

Au niveau international, l'Irlande est reliée au système d'interconnexion des RCB (*Bank Account Registers Interconnection System*, BARIS), qui relie les registres de tous les États membres de l'UE. Les demandes d'accès étrangères doivent être approuvées manuellement par l'administration fiscale irlandaise. Il n'y a pas de possibilité de *data mining* centralisé au niveau européen; chaque État membre conserve son propre accès et son propre logging.

M. Van Quickenborne énumère les points forts du système irlandais ISBAR (*Ireland Safe Deposit Box Bank and Payment Accounts Register*): très haut niveau de qualité des données et rapidité des temps de réponse, gouvernance transparente, délimitation juridique stricte des compétences et respect total des directives européennes anti-blanchiment. Il n'est pas certain que le système appelé à régir le PCC possédera les mêmes qualités.

Les faiblesses du système irlandais sont l'absence de lien direct avec le registre UBO, l'absence de fonctions analytiques et le fait que le système est uniquement hébergé physiquement au sein de l'administration fiscale, sans infrastructure partagée avec la cellule de renseignement financier irlandaise.

Quant à savoir comment le grand public perçoit l'ISBAR, un sondage révèle que 78 % des répondants jugent la législation relative à l'ISBAR nécessaire et équilibrée. L'intervenant demande au ministre comment le PCC est perçu par le grand public en Belgique.

De heer Van Quickenborne licht vervolgens de juridische basis, de institutionele structuur en de governance van het ISBAR toelichten. Het ISBAR is opgericht in 2021 en wordt gekarakteriseerd als juridisch terughoudend. Het systeem werd ingevoerd nadat Ierland in 2019 door de Europese Commissie op de vingers werd getikt omdat de diensten bij elk vermoeden van witwas afzonderlijk contact moesten opnemen met de banken. De spreker merkt op het CAP in België in 2011 werd geïntroduceerd en dat op 8 juli 2018 de wet houdende organisatie van een centraal aanspreekpunt van rekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest werd ingevoerd.

In België wordt het CAP beheerd door de Nationale Bank, terwijl in Ierland de belastingdienst verantwoordelijk is voor het technische en organisatorische beheer van het register. Zij ontvangen de gegevens, voeren kwaliteitscontroles uit en behandelen de toegangs aanvragen. Alleen de informatiegerechtigden kunnen toegang krijgen, en elke raadpleging vereist een geautoriseerde dossiercode en wordt gelogd. Het beheercentrum van de Ierse belastingdienst, de *ISBAR Operations Unit*, bestaat uit twintig medewerkers en beschikt over een budget van 3,2 miljoen euro. Wat is de situatie in België? Het Ierse ministerie van Financiën bepaalt het beleid en legt jaarlijks verantwoording af aan het Ierse parlement. De minister dient een publiek verslag in over de prestaties van het register, de incidenten en de internationale samenwerking. In België vindt deze kennisgeving niet plaats.

Daarnaast houdt de DPC als gegevensbeschermingsautoriteit toezicht op de naleving van de AVG en de *Data Protection Act* van 2018. Zij keurt de *Data Protection Impact Assessment* goed, controleert de logs en kan bindende bevelen uitvaardigen. Volgens een rapport van de DPC uit 2024 geeft het ISBAR blijk van proportionaliteit en hoge technische naleving van de EU-privacyprincipes. Bestaat er een vergelijkbare beoordeling van het CAP door de Belgische Gegevensbeschermingsautoriteit?

De spreker herhaalt dat het ISBAR een beperkt aantal gegevens bevat en dat saldi en transacties uitgesloten zijn. Elke bank moet dagelijks updates sturen naar het *Revenue Online Service* (ROS)-platform. Indien banken dit niet doen, kunnen boetes tot 250.000 euro worden

M. Van Quickenborne commente ensuite le fondement juridique, la structure institutionnelle et la gouvernance de l'ISBAR. Ce système a été créé en 2021 et se caractérise par sa retenue juridique. L'Irlande l'a mis sur pied après avoir été tancée par la Commission européenne en 2019, parce que les services irlandais devaient contacter séparément les banques à chaque suspicion de blanchiment. L'intervenant fait observer que le PCC a été instauré en Belgique en 2011 et que la loi portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt date du 8 juillet 2018.

En Belgique, le PCC est géré par la Banque nationale, tandis qu'en Irlande, c'est l'administration fiscale qui est responsable de la gestion technique et organisationnelle du registre. Celle-ci reçoit les données, procède aux contrôles de qualité et traite les demandes d'accès. Seules les personnes habilitées à recevoir l'information peuvent y accéder, et chaque consultation nécessite un code de dossier autorisé et est journalisée. Le centre de gestion de l'administration fiscale irlandaise, l'*ISBAR Operations Unit*, compte vingt collaborateurs et est doté d'un budget de 3,2 millions d'euros. Quelle est la situation en Belgique? Le ministère irlandais des Finances définit la politique à mener et fait rapport chaque année au Parlement irlandais. Le ministre présente un rapport public sur les résultats du registre, les incidents et la coopération internationale. En Belgique, cette information n'a pas lieu.

En outre, l'autorité de protection des données irlandaise (*Data Protection Commission ou DPC*) veille au respect du RGPD et de la législation relative à la protection des données de 2018 (*Data Protection Act*). Elle approuve l'analyse d'impact relative à la protection des données (*Data Protection Impact Assessment – DPIA*), contrôle les journaux et peut émettre des directives à caractère contraignant. Selon un rapport de la DPC de 2024, l'ISBAR respecte la proportionnalité et affiche un niveau élevé de conformité technique avec les principes de respect de la vie privée de l'Union. Le PCC est-il soumis à une évaluation analogue par l'Autorité belge de protection des données?

L'intervenant répète que l'ISBAR contient un nombre limité de données et que les soldes et les transactions en sont exclus. Chaque banque doit envoyer quotidiennement des mises à jour à la plateforme *Revenue Online Service* (ROS). Si elles omettent de le faire, les banques

opgelegd. In België zijn de boetes hoger, tot 500.000 euro, en worden ze opgelegd door de Thesaurie.

De bewaartermijn in Ierland bedraagt vijf jaar na sluiting van de rekening, waarna de gegevens automatisch verwijderd of geanonimiseerd worden. In België is dit tien jaar. Het ISBAR werkt volgens het principe van *least data necessary*, wat betekent dat enkel de strikt noodzakelijke gegevens worden verzameld.

Wat betreft dataminimalisatie geldt in Ierland het principe van *least data necessary*: er is geen koppeling met commerciële gegevens of kredietregisters.

Met betrekking tot toezicht en verantwoording licht de spreker toe dat elke query wordt geregistreerd met de identiteit van de gebruiker, het doel van de raadpleging, het tijdstip en de resultaatcode. Deze logs worden tien jaar bewaard. In België bedraagt de bewaartermijn van de logs zes maanden. De logs in Ierland worden opgeslagen op een WORM-gegevensdrager (*write once read many*).

Er vinden externe audits plaats. Zo voert de *Office of the Comptroller and Auditor General* jaarlijks een technische en financiële audit uit. De DPC controleert de naleving van de privacyregels. Tot op heden zijn er volgens de DPC geen overtredingen vastgesteld.

De heer Van Quickenborne verwijst vervolgens naar de parlementaire verantwoording in Ierland. Daar bestaat een *Committee on Finance, Public Expenditure and Reform*, die jaarlijks een hoorzitting houdt met de minister van Financiën en de commissaris van de belastingdienst.

Hij besluit dat het Ierse systeem, het ISBAR, een compact maar efficiënt centraal aanspreekpunt is, dat volledig voldoet aan de EU-richtlijnen en de AVG. De sterke punten zijn de dagelijkse updates, het duidelijke verbod op datamining en de strikte toegangscontrole. Hierdoor geldt het systeem als een referentie binnen de *no datamining*-groep van landen.

De heer Van Quickenborne bespreekt vervolgens de functionele werking en het procesbeheer van het ISBAR, zoals hij dit ook bij andere landen heeft gedaan. Het systeem werkt volgens een centrale rapporteringscyclus. Elke financiële instelling uploadt vóór middernacht de relevante updates via het ROS-portaal. De data worden gevalideerd, geconsolideerd en opgeslagen in de ISBAR-database, die binnen de infrastructuur van de Ierse belastingdienst draait. Om zes uur Ierse tijd wordt het register gesynchroniseerd met een raadpleegbare

s'exposent à des amendes allant jusqu'à 250.000 euros. En Belgique, les amendes sont plus élevées, jusqu'à 500.000 euros, et sont infligées par l'Administration générale de la Trésorerie.

En Irlande, le délai de conservation est de cinq ans après la clôture du compte. Passé ce délai, les données sont automatiquement supprimées ou anonymisées. En Belgique, il est fixé à 10 ans. L'ISBAR fonctionne selon le principe *Least data* ou minimisation des données: seules les données strictement nécessaires sont collectées.

Conformément au principe de minimisation précité, l'Irlande n'opère pas de couplage avec des données commerciales ou des registres de crédit.

En ce qui concerne le contrôle et la responsabilité, l'intervenant explique que chaque demande est enregistrée avec l'identité de l'utilisateur, l'objet de la consultation, l'heure et le code du résultat. Ces journaux sont conservés pendant dix ans. En Belgique, ceux-ci sont soumis à un délai de conservation de six mois. En Irlande, les journaux sont stockés sur un support WORM (*write once read many*).

Des audits externes ont également lieu. Ainsi, l'*Office of the Comptroller & Auditor General* procède chaque année à un audit technique et financier. La DPC contrôle le respect des règles en matière de respect de la vie privée et n'a constaté aucune infraction jusqu'à présent.

M. Van Quickenborne renvoie ensuite aux rapports rendus au Parlement irlandais, au sein duquel un *Committee on Finance, Public Expenditure and Reform* auditionne chaque année le ministre des Finances et le commissaire de l'administration fiscale.

L'intervenant en conclut que le système irlandais, l'ISBAR, est un point de contact central à la fois compact et efficace, qui est totalement conforme aux directives de l'Union européenne et au RGPD. Ses points forts sont les mises à jour quotidiennes, l'interdiction formelle du *data mining* et un contrôle d'accès strict. Ces qualités font de ce système une référence parmi le groupe de pays n'appliquant pas le *data mining*.

M. Van Quickenborne décrit ensuite le fonctionnement et la gestion de processus de l'ISBAR, comme il l'a fait pour d'autres pays. Ce système repose sur un cycle de rapportage central. Chaque institution financière téléverse les mises à jour pertinentes avant minuit sur le portail ROS. Les données sont validées, consolidées et stockées dans la base de données ISBAR, qui est hébergée dans l'infrastructure de l'administration fiscale irlandaise. À six heures (heure de Dublin), le registre est synchronisé avec un environnement consultable, de

omgeving, zodat bevoegde autoriteiten altijd toegang hebben tot gegevens die maximaal vierentwintig uur oud zijn.

De heer Van Quickenborne benadrukt het fundamentele verschil met het Belgische systeem: bij ons gaat het CAP de data in het datawarehouse pompen, waardoor slechts een kopie beschikbaar is en niet het origineel. De Gegevensbeschermingsautoriteit waarschuwt dat werken met kopieën kan leiden tot verouderde informatie en een verhoogd risico op vals-positieve resultaten. In Ierland hebben bevoegde autoriteiten dus altijd toegang tot actuele gegevens, wat de nauwkeurigheid aanzienlijk verhoogt.

Het operationele proces in Ierland bestaat uit vijf stappen:

1. *data ingestion*: upload van gegevens door banken via beveiligde API's;
2. validatie: automatische controle van de XML-structuur en van het PPSN-formaat (*Personal Public Service Number*), dat dienstdoet als uniek identificatienummer voor natuurlijke personen;
3. transformatie: normalisatie van gegevens binnen het interne datamodel;
4. indexering van gegevens op PPSN, registratienummer en e-mailadres;
5. replicatie naar back-upservers op twee locaties in Ierland, namelijk Kilcarberry en Portlaoise.

De foutenmarge in Ierland bedraagt minder dan 0,05 %, en foutieve registraties worden automatisch afgekeurd en binnen één dag gecorrigeerd.

De toegang tot het *ISBAR Portal for Authorized Users* verloopt via drie gebruikersprofielen. Voor de vijf bevoegde instanties bestaan er zogenaamde *investigative users*, waaronder het *Criminal Assets Bureau* en de Ierse financiële inlichtingeneenheid. Deze gebruikers hebben de nodige bevoegdheden om operationeel toegang te krijgen tot de gegevens. Daarnaast zijn er de zogenaamde *supervisory users*, waaronder de Ierse centrale bank. Tevens kan ook de politie als *investigative user* optreden. Voor de Ierse belastingdienst zelf bestaat een profiel met administratieve bevoegdheden (*administrative user*).

sorte que les autorités compétentes ont toujours accès à des données qui n'ont pas plus de vingt-quatre heures.

M. Van Quickenborne met l'accent sur la différence fondamentale par rapport au système belge. En Belgique, le PCC va chercher les données contenues dans le *data warehouse*, et ne dispose donc que de copies et non de données originales. L'Autorité de protection des données prévient que l'utilisation de copies peut entraîner l'utilisation d'informations obsolètes et accroître le risque de faux positifs. En Irlande, les autorités compétentes ont donc toujours accès à des données actualisées, ce qui renforce considérablement la précision.

Le processus opérationnel du système irlandais se décompose en cinq étapes:

1. ingestion de données: téléversement de données par les banques au moyen d'API sécurisées;
2. validation: contrôle automatique de la structure XML et du format PPSN (*Personal Public Service Number*), qui fait office de numéro d'identification unique pour les personnes physiques;
3. transformation: normalisation des données dans le cadre du modèle de données interne;
4. indexation des données par PPSN, numéro d'enregistrement et adresse e-mail;
5. réplication vers des serveurs de back-up à deux endroits en Irlande, à savoir à Kilcarberry et Portlaoise.

La marge d'erreur du système irlandais est inférieure à 0,05 %, et les enregistrements erronés sont automatiquement rejetés et corrigés dans la journée.

L'accès au portail *ISBAR* destiné aux utilisateurs autorisés (*ISBAR Portal for Authorized Users*) est accordé sur la base de trois profils d'utilisateurs. Pour les cinq instances compétentes, il existe un profil pour les utilisateurs qui enquêtent (*investigative users*), entre autres pour l'Agence de dépistage des avoirs criminels (*Criminal Assets Bureau*) et la Cellule de renseignement financier. Ces utilisateurs ont les compétences nécessaires pour obtenir un accès opérationnel aux données. Il existe aussi un profil pour les utilisateurs chargés de la surveillance (*supervisory users*), dont fait partie la Banque centrale irlandaise. La police peut également agir en tant qu'utilisateur qui enquête. Enfin, un profil d'utilisateur administratif (*administrative user*) est prévu pour l'administration fiscale.

Elke raadpleging wordt automatisch gelogd met gebruikers-ID, doel van de raadpleging en tijdstempel. De Ierse gegevensbeschermingsautoriteit (*Data Protection Commission* – DPC) heeft read-only toegang tot de logdatabase en voert steekproefsgewijze controles uit. Dit vormt de functionele werking van het procesbeheer.

De spreker licht vervolgens de toezichtstructuur en de onafhankelijkheid van het Ierse systeem toe.

Ten eerste is er de DPC, een onafhankelijke toezichthouder, die de rechtmatigheid van de gegevensverwerking, de naleving van loggingprocedures en incidentmeldingen en klachten beoordeelt. Het jaarverslag van 2024 vermeldt geen overtredingen en classificeert het ISBAR als proportioneel en correct ingericht.

Daarnaast is er de *Comptroller and Audit General* (CAG), een typisch Angelsaksisch orgaan dat het financiële beheer en de IT-beveiliging controleert. De CAG heeft bevestigd dat het Ierse systeem cyberveilig functioneert en conform de regelgeving is.

De heer Van Quickenborne vergelijkt dit met België en merkt op dat het CAP hier niet dezelfde transparantie en jaarlijkse verificatie kent.

Ten slotte is er de parlementaire controle. In Ierland organiseert de zogenaamde *Committee on Finance, Public Expenditure and Reform* jaarlijks een openbare zitting met de minister van Financiën en de Ierse belastingdienst. De voorzitter van de Ierse belastingdienst moet jaarlijks verantwoording afleggen aan het Ierse Parlement.

In België wordt het CAP daarentegen niet jaarlijks geëvalueerd. De spreker stelt voor dat het gebruik van het CAP jaarlijks wordt onderzocht, inclusief de toegangscijfers en eventuele datalekken. Momenteel zijn daarover geen cijfers beschikbaar. Wel zijn cijfers over het aantal raadplegingen terug te vinden op de website van de Kamer. Daarnaast werd in de media aandacht besteed aan dit onderwerp.

Naast het toezicht door de DPC, de CAG en het parlement, bestaat er in Ierland ook gerechtelijk toezicht. Indien de Ierse financiële inlichtingeneenheid of de politie gegevens uit het ISBAR wil gebruiken, is een gerechtelijk bevel vereist. In België kan justitie het CAP consulteren zonder gerechtelijk bevel, hoewel dit uiteraard binnen de grenzen van aanwijzingen van criminaliteit dient te gebeuren. In Ierland houdt de *High Court* toezicht op de proportionaliteit van deze bevelen.

Chaque consultation est automatiquement enregistrée dans un journal, avec l'identifiant de l'utilisateur, de la finalité de la consultation et de l'horodatage. L'autorité irlandaise de protection des données (*Data Protection Commission*, DPC) dispose d'un accès en lecture seule à la banque de données du journal et effectue des contrôles par échantillonnage. Telle est l'organisation fonctionnelle de la gestion des processus.

L'intervenant présente ensuite la structure de contrôle et l'indépendance du système irlandais.

Tout d'abord, l'autorité de contrôle indépendante DPC évalue la légalité du traitement de données, le respect des procédures de journalisation, ainsi que les signalements d'incidents et les plaintes. Le rapport annuel 2024 de la DPC ne mentionne aucune infraction et présente l'ISBAR comme étant proportionné et correctement organisé.

À cela s'ajoute le CAG (*Comptroller and Audit General*), qui est un organe typiquement anglo-saxon qui contrôle la gestion financière et la protection informatique. Le CAG a confirmé que le système irlandais fonctionnait d'une manière cybersécurisée et conforme à la réglementation.

M. Van Quickenborne fait la comparaison avec la Belgique, puis observe que le PCC n'offre pas le même degré de transparence et de vérification annuelle.

Enfin, dans le cadre du contrôle parlementaire, la commission des Finances, des Dépenses publiques et des Réformes (*Committee on Finance, Public Expenditure and Reform*) organise une réunion publique annuelle à laquelle participent le ministre des Finances et l'administration fiscale irlandaise, dont le président doit faire annuellement rapport au Parlement irlandais.

En Belgique, par contre, le PCC n'est pas évalué chaque année. L'intervenant propose que l'utilisation du PCC fasse l'objet d'un examen annuel qui porterait également sur les chiffres d'accès et les éventuelles fuites de données. À l'heure actuelle, aucun chiffre n'est disponible à ce sujet. Des statistiques sur le nombre de consultations peuvent néanmoins être consultées sur le site web de la Chambre. Par ailleurs, les médias se sont intéressés à cette question.

Outre la surveillance exercée par le DPC, le CAG et le Parlement, l'Irlande dispose également d'un contrôle judiciaire. Si l'unité irlandaise de renseignement financier ou la police souhaite utiliser des données issues de l'ISBAR, un mandat judiciaire est nécessaire. En Belgique, la justice peut consulter le CAP sans mandat judiciaire, bien que cela doive bien sûr se faire dans les limites des indications de criminalité. En Irlande, la Haute Cour supervise la proportionnalité de ces mandats.

Wat betreft de samenwerking met de banken en instellingen in Ierland deelt de heer Van Quickenborne mee dat het ISBAR meerdere afzonderlijke informatieverzoeken vervangt. De *Banking and Payment Federation of Ireland (BPFI)* pleegt overleg met de Ierse belastingdienst en de Ierse centrale bank over technische standaarden. Heeft de minister reeds overleg gehad met Febelfin, de Belgische tegenhanger van het BPFI, over het CAP en wat werd tijdens dat overleg besproken?

Technisch gezien ontwikkelden de BPFI en de Ierse Belastingdienst gezamenlijk een open standaard voor gegevensuitwisseling, het zogenaamde *ISBAR XML Schema 2.1*. Elke Ierse bank beschikt bovendien over een *ISBAR Compliance Officer*, verantwoordelijk voor de dagelijkse aanlevering van gegevens. Werken banken in België eveneens met *CAP Compliance Officers* en hoe wordt dat juist georganiseerd?

In Ierland kan de Ierse belastingdienst bij niet-naleving administratieve sancties opleggen tot 250.000 euro. Bij herhaalde fouten kan melding worden gemaakt aan de Ierse centrale bank. In 2024 werd geen enkele zware overtreding vastgesteld.

Wat betreft de bescherming van gegevens en privacy-waarborgen wijst de spreker erop dat Ierland als lidstaat van de Europese Unie strikt toeziet op de naleving van de *Data Protection Impact Assessments (DPIA's)*. Voor de ingebruikname van het ISBAR werd een DPIA uitgevoerd door de Ierse belastingdienst en goedgekeurd onder de voorwaarden van *Strict Purpose Limitation* (doelbinding), *Automated Access Control* (geautomatiseerde toegang) en *Prohibition of Cross-Matching with Other Datasets* (geen datamining of koppeling met andere datasets).

Het systeem is ontworpen volgens het principe van *privacy by design*, met minimale datavelden, encryptie, een beperkte bewaartermijn van vijf jaar en dubbele autorisatie bij toegang. Wettelijk is vastgelegd dat *no automated analysis, datamining or profiling shall be carried out using the centralised bank account register*. Dit maakt Ierland tot een van de meest privacy gerichte lidstaten van de Europese Unie.

De heer Van Quickenborne vraagt of de minister ooit overleg heeft gehad met zijn voormalige collega Paschal

En ce qui concerne la coopération avec les banques et les institutions en Irlande, M. Van Quickenborne précise que l'ISBAR permet de remplacer plusieurs demandes d'informations distinctes. Une concertation portant sur les normes techniques est organisée entre la BPFI (*Banking and Payment Federation of Ireland*), l'administration fiscale irlandaise et la Banque centrale d'Irlande. Le ministre s'est-il déjà concerté avec Febelfin, l'équivalent de la BPFI en Belgique, à propos du PCC et, si oui, quel a été l'objet de cette concertation?

Sur le plan technique, la BPFI et l'administration fiscale irlandaise ont développé ensemble une norme ouverte d'échange de données baptisée *ISBAR XML Schema 2.1*. En outre, dans chaque banque irlandaise, un *ISBAR Compliance Officer* est responsable de la transmission quotidienne des données. Les banques belges ont-elles aussi des *PCC Compliance Officers*, et comment est-ce organisé exactement?

En Irlande, l'administration fiscale peut infliger des amendes administratives qui peuvent atteindre 250.000 euros en cas de non-respect. Un signalement peut aussi être adressé à la Banque centrale d'Irlande en cas d'erreurs répétées. En 2024, aucune infraction grave n'a été constatée.

En ce qui concerne la protection des données et les garanties de respect de la vie privée, l'intervenant indique que l'Irlande, en tant qu'État membre de l'Union européenne, veille scrupuleusement au respect des analyses d'impact relatives à la protection des données (AIPD). Avant la mise en service de l'ISBAR, une AIPD a été effectuée par l'administration fiscale irlandaise et approuvée sous les conditions de limitation stricte de finalité (*Strict Purpose Limitation*), de contrôle d'accès automatisé (*Automated Access Control*) et d'interdiction de *data mining* et de recoupement avec d'autres ensembles de données (*Prohibition of Cross-Matching with Other Datasets*).

Ce système a été conçu selon le principe de protection de la vie privée dès la conception (*privacy by design*), en prévoyant des champs de données minimalistes, le cryptage des données, un délai de conservation limité à cinq ans et un accès soumis à une double autorisation. Par ailleurs, la législation irlandaise prévoit qu'aucune forme automatisée d'analyse, de *data mining* ou de profilage ne peut être réalisée à l'aide du registre centralisé des comptes bancaires. L'Irlande fait ainsi partie des États membres de l'Union européenne qui se soucient le plus du respect de la vie privée.

M. Van Quickenborne demande au ministre s'il s'est déjà entretenu avec son ancien collègue, M. Paschal

Donahoe over het Ierse CAP of over de Belgische plannen voor *money control*.

De minister bevestigt dat dit niet het geval is, noch met andere ministers van Financiën.

Wat betreft de internationale context en evaluatie van het systeem merkt *de heer Van Quickenborne* op dat het ISBAR sinds 2023 is aangesloten op het Europese interconnectiesysteem, als uitvoering van de CRS-richtlijn. Logregistratie en controle door de DPC blijven Iers. Een evaluatie door de Europese Commissie in het *AML Implementation Report 2024* waardeerde Ierland als volledig conform artikel 32a van de vierde anti-witwasrichtlijn van 2015. De Commissie prijst het privacybewuste beheer en de minimale dataverwerking.

De internationale samenwerking verloopt via de *Financial Intelligence Unit* (FIU), wat de Ierse variant is van de Belgische CFI, die informatie enkel deelt met individuele toestemming van de minister van Justitie. Systematische datakoppeling op internationaal niveau wordt vermeden.

Dagelijks worden in Ierland ongeveer 45.000 registraties opgeladen. De foutenmarge bedraagt minder dan 0,1 %, en er zijn geen onrechtmatige toegangen vastgesteld. De gemiddelde respons bij een opvraging van bankgegevens via het ISBAR bedroeg aanvankelijk 48 uur en is teruggebracht tot minder dan 30 seconden. Daaruit blijkt duidelijk de efficiëntie van het Ierse systeem. Bovendien kan het *Criminal Assets Bureau* witwasonderzoeken sneller uitvoeren, hetgeen de bestrijding van criminaliteit ten goede komt.

De belangrijkste beperking is het ontbreken van real-time integratie met de banken. Macrostatistische analyses kunnen niet worden uitgevoerd vanwege het dataminingsverbod. Dit vormt een nadeel, aangezien het onmogelijk maakt uitgebreide statistische inzichten te ontwikkelen. Dit betekent echter een mogelijk voordeel ten aanzien van een systeem zoals *money control*, waarbij grotere analysecapaciteit bestaat.

Jaarlijks wordt een *ISBAR activity report* gepubliceerd, met geanonimiseerde statistieken. Deze transparantie versterkt het publieke vertrouwen. Ongeveer 76 % van de Ierse bevolking steunt het systeem, terwijl slechts 12 % misbruik door de overheid vreest. De Ierse pers heeft het ISBAR beschreven als een model van *light-touch surveillance*, dat gericht, proportioneel en transparant

Donahoe, au sujet du PCC irlandais ou des projets belges de *money control*.

Le ministre répond qu'il ne s'est entretenu ni avec lui, ni avec d'autres ministres des Finances.

En ce qui concerne le contexte international et l'évaluation du système, *M. Van Quickenborne* fait observer qu'en application de la directive CRS, l'ISBAR est rattaché au système d'interconnexion européen depuis 2023. La journalisation et les contrôles réalisés par la DPC restent nationaux. Dans le cadre de l'une de ses évaluations (*AML Implementation Report 2024*), la Commission européenne a estimé que l'Irlande se conformait pleinement à l'article 32 de la quatrième directive anti-blanchiment de 2015. La Commission a félicité l'Irlande pour sa gestion respectueuse de la vie privée et son traitement minimal des données.

La *Financial Intelligence Unit* (FIU) – le pendant irlandais de la CTIF en Belgique – se charge de la coopération internationale et ne communique des informations qu'avec l'autorisation expresse du ministre de la Justice. Tout couplage systématique des données au niveau international est évité.

Chaque jour, l'Irlande procède à quelque 45.000 enregistrements. La marge d'erreur est inférieure à 0,1 % et aucun accès illicite n'a été constaté jusqu'à présent. Le temps de réponse moyen à une demande de données bancaires via l'ISBAR ne dépasse pas les 30 secondes alors qu'il était initialement de 48 heures. Ces chiffres démontrent clairement l'efficacité du système irlandais. En outre, le *Criminal Assets Bureau* (Bureau irlandais des avoirs d'origine criminelle) peut enquêter plus rapidement sur le blanchiment d'argent, ce qui contribue à la lutte contre la criminalité.

Le principal point négatif du système irlandais est l'absence d'intégration en temps réel avec les banques. Le *data mining* étant interdit, il n'est pas possible de procéder à des analyses macrostatistiques. Il s'agit d'un inconvénient, car ce système ne permet pas de fournir des connaissances statistiques approfondies. L'intervenant y voit toutefois un certain avantage par rapport à un système tel que le *money control*, qui générera une plus grande capacité d'analyse.

Chaque année, l'ISBAR fait l'objet d'un rapport d'activité contenant des statistiques anonymisées. Cette transparence renforce la confiance du public. Environ 76 % de la population irlandaise est favorable au système, alors que seulement 12 % des Irlandais craignent des abus de la part des pouvoirs publics. La presse irlandaise a décrit l'ISBAR comme un modèle de surveillance

is. In 2024 stelde de *Irish Times* dat Ierland aantoonde dat financiële transparantie en privacy elkaar niet uitsluiten.

De heer Van Quickenborne concludeert dat het ISBAR een stabiel, efficiënt en juridisch goed uitgebalanceerd systeem is. Het voldoet aan alle EU-verplichtingen zonder datamining toe te laten en bewijst dat een modern financieel register kan functioneren binnen een strikte privacywetgeving.

Wat de technische werking en de operationele structuur betreft, merkt hij op dat het ISBAR een van de technisch meest gestroomlijnde, maar juridisch strengst gereguleerde registers van Europa is. Het systeem werd ontworpen in 2021 als lichtgewicht en combineert een hoogbeveiligde infrastructuur met maximale efficiëntie en minimale gegevensverwerking. De kernfilosofie van de ontwerpers luidt: *as much functionality as necessary, as little data as possible*, oftewel: zo efficiënt mogelijk en met zo weinig mogelijk data.

De heer Van Quickenborne geeft aan dat het Ierse systeem niet alleen performant is, maar ook volledig strookt met de Europese privacywetgeving.

Het Ierse systeem bestaat uit vier geïntegreerde componenten.

De eerste is de *data ingestion layer*, de interface waar banken en betalingsinstellingen hun gegevens uploaden via het *Revenue Online Service*-platform. Ten tweede is er de *core database*, de centrale versleutelde databank binnen de infrastructuur. Ten derde is er de *access gateway*, de *ISBAR-query-engine*, die fungeert als beveiligde toegangspoort voor bevoegde autoriteiten om informatie te consulteren. Het vierde element is de audit- en compliance-module, een onafhankelijk subsysteem dat logging, toezicht en rapportage beheert. De vier lagen communiceren via beveiligde API's (*Application Programming Interface*) binnen het interne overheidsnetwerk *GovNet Ireland* en zijn volledig gescheiden van het publieke internet.

Het interne datamodel is bewust minimaal en omvat veertien velden, waaronder het PPSN, het rijksregisternummer, het IBAN, het bank-ID, de datum van opening en sluiting, en de gemachtigden. De structuur is genormaliseerd om redundantie te vermijden, en elke registratie wordt geïndexeerd op PPSN en IBAN. Hierdoor kan een

moderée, ciblé, proportionnée et transparente. En 2024, le quotidien *Irish Times* a souligné que l'Irlande était la preuve que la transparence financière et la vie privée n'étaient pas incompatibles.

M. Van Quickenborne conclut que l'ISBAR est un système stable, efficace et juridiquement équilibré. Il satisfait à toutes les obligations européennes sans autoriser le *data mining* et démontre qu'un registre financier moderne peut fonctionner dans le cadre d'une législation stricte en matière de protection de la vie privée.

En ce qui concerne le fonctionnement technique et la structure opérationnelle, il relève que l'ISBAR est l'un des registres les plus rationalisés sur le plan technique, mais aussi l'un des plus strictement réglementés d'Europe sur le plan juridique. Le système a été conçu en 2021 comme un dispositif léger, combinant une infrastructure hautement sécurisée avec une efficacité maximale et un traitement minimal des données. La philosophie centrale de ses concepteurs est la suivante: *as much functionality as necessary, as little data as possible*, autrement dit: un maximum de fonctionnalité avec un minimum de données.

M. Van Quickenborne indique que le système irlandais n'est pas seulement performant, mais qu'il est aussi totalement conforme à la législation européenne en matière de protection de la vie privée.

Le système irlandais se compose de quatre éléments intégrés.

Le premier est la *data ingestion layer*, l'interface par laquelle les banques et les établissements de paiement téléchargent leurs données au travers de la plateforme *Revenue Online Service*. Le deuxième est la *core database*, la banque de données centrale cryptée au cœur de l'infrastructure. Le troisième est l'*access gateway*, le moteur de requête ISBAR, qui sert de portail sécurisé permettant aux autorités compétentes de consulter des informations. Le quatrième élément est le module d'audit et de conformité, un sous-système indépendant qui gère la journalisation, le contrôle et le *reporting*. Les quatre couches communiquent au moyen d'API (*Application Programming Interface*) sécurisées au sein du réseau gouvernemental interne *GovNet Ireland* et sont totalement distinctes de l'Internet public.

Le modèle de données interne est volontairement minimal et comprend quatorze champs, dont le PPSN, le numéro de registre national, l'IBAN, l'identifiant bancaire, la date d'ouverture et de clôture ainsi que les mandataires. La structure est normalisée afin d'éviter les redondances, et chaque enregistrement est indexé

zoekopdracht doorgaans in minder dan een seconde worden uitgevoerd.

Wat betreft beheer en hosting, merkt de spreker op dat het systeem draait op twee beveiligde datacenters: het *Revenue Datacenter* in Kilcarberry en een disaster recovery-site in Portlaoise. Tussen beide locaties vindt volledige *active replication* plaats. De infrastructuur draait op *Linux Red Hat Enterprise*, en alle code wordt intern onderhouden door een IT-departement van de Ierse belastingdienst.

De heer Van Quickenborne vervolgt dat in Ierland 90 instellingen, waaronder banken en betalingsinstellingen, wettelijk verplicht zijn dagelijks een geüpdatete dataset aan te leveren. Per dag betreft dit circa 45.000 registraties. De dataset wordt aangeleverd in XML-formaat, compatibel met de EU-standaard, en omvat identificatie van de instelling, actieve rekeningen, houders- en gemachtigden, en de openings- en sluitingsdatum van de rekeningen.

Bij ontvangst van de gegevens worden drie controles toegepast: syntax-controle, conformiteit met het XML-schema, een semantische controle, bijvoorbeeld om te verifiëren of de openingsdatum vóór de sluitingsdatum ligt, en een identiteitscontrole binnen het Ierse systeem. Die laatste controle houdt in dat het PPSN, het rijksregisternummer en het KBO-nummer van bedrijven worden gecontroleerd en gekruist met de relevante registers. Fouten worden automatisch gerapporteerd aan de betreffende bank via het feedbackmechanisme. De foutenmarge bedraagt minder dan 0,05 %.

Na de eerste stap van rapportering volgt de validatie. Vervolgens vindt de datatransformatie plaats, waarbij de gegevens worden opgenomen in het interne ISBAR-datamodel en de *Core Database*. Deze verwerking gebeurt dagelijks.

De toegangsstructuur kent drie gebruikerscategorieën: *investigative users*, *supervisory users* en *administrative users*. Afhankelijk van de gebruikersrol verschillen de toegangsrechten. Zo hebben *investigative users*, waaronder de politie, het *Criminal Assets Bureau* en de Ierse financiële inlichtingeneenheid, toegang tot zoekopdrachten op individuen of entiteiten. De Ierse belastingdiensten hebben primair beheerrechten zonder zoekfunctionaliteit. Alle toegang verloopt via tweefactorauthenticatie met het *Revenue Secure Token System*.

sur le PPSN et l'IBAN. De ce fait, une requête peut généralement être exécutée en moins d'une seconde.

En ce qui concerne la gestion et l'hébergement, l'intervenant souligne que le système fonctionne sur deux centres de données sécurisés: le *Revenue Datacenter* à Kilcarberry et un site de reprise après sinistre à Portlaoise. Une réplication active complète (*active replication*) a lieu entre les deux sites. L'infrastructure fonctionne sous *Linux Red Hat Enterprise*, et la maintenance du code est intégralement gérée en interne par un département informatique du fisc irlandais.

M. Van Quickenborne poursuit en indiquant qu'en Irlande, 90 institutions, parmi lesquelles des banques et des établissements de paiement, sont légalement tenues de fournir chaque jour un jeu de données actualisé, ce qui représente environ 45.000 enregistrements par jour. Le jeu de données est transmis au format XML, compatible avec la norme européenne, et comprend l'identification de l'institution, les comptes actifs, les titulaires et les mandataires, ainsi que la date d'ouverture et de clôture des comptes.

Dès la réception des données, trois contrôles sont exécutés: un contrôle de syntaxe, c.-à-d. une vérification de conformité avec le schéma XML, un contrôle sémantique – par exemple pour vérifier si la date d'ouverture précède la date de clôture – et un contrôle d'identité au sein du système irlandais. Ce dernier contrôle consiste à vérifier le PPSN, le numéro de registre national et le numéro BCE des entreprises, en les croisant avec les registres pertinents. Les erreurs sont automatiquement signalées à la banque concernée grâce au mécanisme de retour d'information. La marge d'erreur est inférieure à 0,05 %.

La première étape, qui est celle du *reporting*, précède celle de la validation. Celle-ci est suivie de la transformation des données, par laquelle celles-ci sont intégrées dans le modèle de données interne de l'ISBAR et dans la banque de données centrale (*Core Database*). Ce traitement a lieu quotidiennement.

La structure d'accès distingue trois catégories d'utilisateurs: *investigative users*, *supervisory users* et *administrative users*. Les droits d'accès varient selon le rôle de l'utilisateur. Ainsi, les *investigative users*, au rang desquels figurent la police, le *Criminal Assets Bureau* et l'unité de renseignement financier irlandaise, peuvent effectuer des recherches sur des individus ou des entités. Les services fiscaux irlandais disposent principalement de droits de gestion sans fonctionnalité de recherche. Tous les accès se font au moyen d'une authentification à deux facteurs avec le *Revenue Secure Token System*.

Het systeem van raadpleging werkt via query's op PPSN of IBAN. De gebruiker ontvangt een *read-only result set*, die niet kan worden geëxporteerd en automatisch vervalt na zestig minuten. Elke opzoeking wordt gelogd in de audit- en compliance-module, inclusief gebruikers-ID, IP-adres, tijdstip, dossier en status (voltooid of geweigerd). Deze logs worden opgeslagen op WORM-gegevensdragers (*write once read many*) en jaarlijks gecontroleerd door de DPC.

De heer Van Quickenborne bespreekt vervolgens de beveiligingsarchitectuur van het Ierse systeem. Hij licht toe dat het ISBAR werkt volgens een zogenaamde *defense-in-depth*-architectuur en beschikt over meerdere lagen, waaronder een netwerklaag en een encryptielaag. Alle gegevens worden versleuteld. Over een gelijkaardige encryptie binnen het Belgische CAP-systeem is geen publieke informatie teruggevonden.

Het Ierse systeem omvat daarnaast authenticatie, waaronder biometrische verificatie voor toegang tot fysieke diensten. Verder is er een auditlaag die automatische detectie van ongeoorloofde query's mogelijk maakt via het *Revenue Intrusion Monitoring System* (RIMS). Tot op heden zijn geen incidenten van datalekken of ongeautoriseerde toegang gerapporteerd.

In Ierland worden de gegevens versleuteld met AES256 in Rust en TLS1.3 tijdens de transmissie. De sleutels worden beheerd via een *hardware security module*, in samenwerking met de Ierse centrale bank. De Ierse belastingdiensten beschikt uitsluitend over tijdelijke sessiesleutels, niet over *master keys*. Het systeem volgt het *privacy by design*-principe: minimale dataopslag, automatische verwijdering na vijf jaar, geen ongeautoriseerde replicatie en scheiding tussen functionele data en auditdata. De DPC voerde in 2023-2024 audits uit en bevestigde de conformiteit.

De interne organisatie van het ISBAR omvat twintig personeelsleden verdeeld over drie afdelingen: *Data Operations* (dagelijkse verwerking en validatie), *Compliance and Security* (toegang en beheer) en *Policy & Liaison* (relaties met banken en EU-instellingen). De interne auditdienst van de Ierse belastingdienst controleert de gegevensintegriteit, toeganglogs en naleving van procedurevoorschriften. Rapporten worden gedeeld met het ministerie van Financiën en de DPC. Daarnaast voert de CAG en de *Office of the Government Chief Information Officer* (OGCIO) jaarlijkse technische audits uit. De resultaten van 2024 bevestigen dat het ISBAR

Le système de consultation fonctionne par requêtes sur le PPSN ou l'IBAN. L'utilisateur reçoit un ensemble de résultats en lecture seule, qui ne peut pas être exporté et qui expire automatiquement après soixante minutes. Chaque recherche est consignée dans le module d'audit et de conformité, y compris l'identifiant de l'utilisateur, l'adresse IP, l'heure, le dossier et le statut (terminé ou refusé). Ces journaux sont stockés sur des supports de données WORM (*write once read many*) et contrôlés chaque année par la DPC.

M. Van Quickenborne aborde ensuite l'architecture de sécurité du système irlandais. Il explique que l'ISBAR fonctionne selon une architecture dite *defense-in-depth* et comporte plusieurs couches, dont une couche réseau et une couche de cryptage. Toutes les données sont cryptées. Il semble n'exister aucune information publique quant à l'existence d'un cryptage similaire dans le PCC belge.

Le système irlandais comprend en outre une authentification, notamment une vérification biométrique pour l'accès aux services physiques. Il existe également une couche d'audit qui permet de détecter automatiquement les requêtes non autorisées au moyen du *Revenue Intrusion Monitoring System* (RIMS). À ce jour, aucun incident de fuite de données ou d'accès non autorisé n'a été signalé.

En Irlande, les données sont, lors de leur transmission, cryptées à l'aide de l'algorithme AES-256 implémenté en langage Rust, et protégées par le protocole TLS 1.3. Les clés sont administrées au moyen d'un module matériel de sécurité (*hardware security module*), en collaboration avec la banque centrale irlandaise. L'administration fiscale irlandaise ne dispose que de clés de session temporaires et non de clés "passe-partout". Le système suit le principe *privacy by design*: stockage minimal des données, suppression automatique après cinq ans, absence de répliquon non autorisée et séparation entre données fonctionnelles et données d'audit. La DPC a réalisé des audits en 2023-2024, qui ont conclu à la conformité du système.

L'organisation interne de l'ISBAR comprend vingt membres du personnel répartis en trois départements: *Data Operations* (traitement et validation quotidiens), *Compliance and Security* (accès et gestion) et *Policy & Liaison* (relations avec les banques et les institutions européennes). Le service d'audit interne de l'administration fiscale irlandaise contrôle l'intégrité des données, les journaux d'accès et le respect des prescriptions procédurales. Les rapports sont communiqués au ministère des Finances et à la DPC. En outre, l'AAC et l'*Office of the Government Chief Information Officer* (OGCIO) réalisent chaque année des audits techniques. Les résultats

werkt volgens voorbeeldige standaarden van gegeven-sintegriteit en operationele controle.

Wat betreft internationale interoperabiliteit is het ISBAR aangesloten op het netwerk Baris en deelt vertrouwelijke informatie via de *Egmont Groupe*, die de financiële in-lichtingeneenheden wereldwijd verenigt. De uitwisseling van gegevens vindt uitsluitend plaats onder het principe van wederkerigheid en blijft onder nationale jurisdictie.

Het ISBAR ondersteunt ook de *Common Reporting Standards* (CRS) en de FATCA-processen ondersteunt, al is er geen automatische koppeling tussen het ISBAR en CRS- of FATCA-gegevens.

Wat betreft cyberweerbaarheid voert Ierland een *Security Incident Response Plan* (SIRP) uit. Detectie vindt plaats via het *Revenue Intrusion Monitoring System* (RIMS). Verdachte accounts worden onmiddellijk ge-blokkeerd, de DPC wordt binnen 24 uur geïnformeerd en binnen 72 uur wordt een volledige forensische audit uitgevoerd. Alle gebruikers van ISBAR volgen jaarlijks een opleiding gegevensveiligheid en ethiek, die onder meer AVG, cyberdreigingen en meldingsprocedures behandelt. Back-ups worden elke vier uur gemaakt en dertig dagen bewaard. In geval van uitval kan de back-upsite het systeem binnen vijftien minuten volledig overnemen.

Het systeem is technologisch compact, veilig en vol-ledig privacyconform. Encryptie, minimale dataopslag en een strikte audit zorgen ervoor dat ISBAR een voor-beeld vormt van digitale efficiëntie met respect voor de burgerrechten.

De heer Van Quickenborne licht vervolgens de ope-rationele werkprocessen toe. De dagelijkse datacyclus van ISBAR is volledig geautomatiseerd, maar menselijk gecontroleerd. Het systeem valideert bestanden, voert dubbele controles uit en synchroniseert de kerndatabase tegen zes uur Ierse tijd. Afwijkingen worden automatisch gerapporteerd aan de *ISBAR Operations Unit*, die elke ochtend een kwaliteitscontrole uitvoert op 0,5 % van de records. Mogelijke afwijkingen betreffen onder meer dubbele IBAN-nummers, foutieve PPSN's, onbestaande reeksnummers en ontbrekende sluitingsdata. Fouten worden teruggestuurd naar de betrokken instelling voor correctie. Het foutenpercentage bedraagt circa 0,05 %, uitzonderlijk laag binnen de EU-context.

de 2024 confirment que l'ISBAR fonctionne selon des normes de référence exemplaires en matière d'intégrité des données et de contrôle opérationnel.

En ce qui concerne l'interopérabilité internationale, l'ISBAR est connecté au réseau *Baris* et partage des informations confidentielles par l'intermédiaire du Groupe Egmont, qui réunit les cellules de renseignement finan-cier dans le monde entier. L'échange de données se fait exclusivement selon le principe de réciprocité et reste sous juridiction nationale.

L'ISBAR prend également en charge les *Common Reporting Standards* (CRS) et les processus FATCA (*Foreign Account Tax Compliance*), bien qu'il n'existe aucun couplage automatique entre l'ISBAR et les don-nées CRS ou FATCA.

En ce qui concerne la cyberrésilience, l'Irlande ap-plique un *Security Incident Response Plan* (SIRP). Les détections se font à l'aide du *Revenue Intrusion Monitoring System* (RIMS). Les comptes suspects sont immédiatement bloqués, la DPC est informée dans les 24 heures et un audit légal complet est effectué dans les 72 heures. Tous les utilisateurs du registre ISBAR suivent chaque année une formation axée sur la sécurité des données et l'éthique qui aborde notamment le RGPD, les cybermenaces et les procédures de signalement. Des back-ups sont effectués toutes les quatre heures et conservés pendant trente jours. En cas de crash, le site back-up est à même de rétablir l'intégralité du système dans les quinze minutes.

La technologie du système est compacte, sécurisée et entièrement conforme aux règles de protection de la vie privée. Le chiffrement, le stockage minimal de données et un audit strict font du registre ISBAR un modèle d'efficacité numérique et de respect des droits des citoyens.

M. Van Quickenborne commente ensuite les proces-sus opérationnels. Le cycle quotidien des données du registre ISBAR est entièrement automatisé, mais reste soumis à une vigilance humaine. Le système valide les fichiers, mène des contrôles doubles et synchronise la banque de données centrale à six heures, heure irlandaise. Lorsqu'une anomalie est détectée, elle est automatiquement communiquée à l'*ISBAR Operations Unit*, qui effectue tous les matins un contrôle de qualité sur 0,5 % des dossiers. Les anomalies peuvent notamment provenir de doubles numéros IBAN, de numéros PPSN erronés, de numéros de série inexistantes et de données de clôture manquantes. Les erreurs sont renvoyées à l'établissement concerné pour correction. Le taux d'erreur se monte à environ 0,05 % et est donc particulièrement faible par rapport aux autres pays européens.

Bevoegde autoriteiten hebben snelle toegang tot het systeem. De gemiddelde responstijd bedraagt minder dan 40 seconden. Authenticatie vindt plaats via twee factoren, inclusief een onderzoekscode (*case reference ID*). De query wordt vergeleken met het toegangsregister en het resultaat toont het rekeningnummer en de openings- of sluitingsdatum. Elke query wordt automatisch gevalideerd op rechtmatigheid. Ongeautoriseerde pogingen worden in real-time gemeld aan het *Security and Compliance Team*. De DPC heeft continue read-only toegang tot de logs.

Datamining is in Ierland verboden. Interne risico-classificatie vindt plaats via vier niveaus (R1–R4), waarbij R4 staat voor hoog risico, zoals terrorisme. Resultaten worden gecontroleerd volgens het vierogen-principe. Er worden geen algoritmen voor patroonherkenning of automatische correlatie gebruikt; juridische proportionaliteit en traceerbaarheid van beslissingen zijn centraal.

De DPC voert halfjaarlijkse controles uit op de querylogs. In 2024 werden vier waarschuwingen gegeven wegens te brede zoekcriteria; er zijn geen ernstige overtredingen vastgesteld. Het ISBAR-rapport 2024 vermeldt een gemiddelde responstijd van 77 seconden, zonder ongeoorloofde toegang of datalekken.

Betreffende de samenwerking tussen het ISBAR en de banksector, verduidelijkt de spreker dat elke bank beschikt over een zogenaamde *ISBAR Compliance Officer*, verantwoordelijk voor tijdige uploads en correcte gegevensaanlevering. Bij niet-naleving kunnen boetes worden opgelegd tot 250.000 euro en kan een melding worden gedaan aan de Ierse centrale bank.

Er bestaat een regelmatig overleg met de banken, de *Banking and Payments Federation of Ireland* (BPF). Dit overleg betreft onder meer technische standaarden en implementatie van het ISBAR XML Schema 2.1, dat door alle instellingen wordt toegepast. Updates verlopen via beveiligde API's met TLS 1.3. Sinds 2024 is ook de ondersteuning voor *e-money providers* verplicht.

Het Ierse model bevordert co-regulering: de private sector levert nauwkeurige data, terwijl de staat de toegang en privacy handhaaft. Dit resulteert in een zeer hoge nalevingsgraad van meer dan 99,9 %.

Les autorités compétentes ont un accès rapide au système. Le temps de réponse moyen se monte à moins de 40 secondes. L'authentification s'effectue à l'aide de deux facteurs, dont l'un est un code d'enquête (*case reference ID*). La requête est comparée avec le registre d'accès et le résultat affiche le numéro de compte et la date d'ouverture et de clôture. La validité de chaque requête est validée automatiquement. Les tentatives non autorisées sont signalées en temps réel à la *Security and Compliance Team*. La DPC a un accès permanent en lecture seule aux journaux.

L'Irlande interdit le *data mining*. La classification de risque interne comprend quatre niveaux (R1–R4), R4 étant le risque le plus élevé, notamment le risque de terrorisme. Les résultats sont contrôlés selon le principe des quatre yeux. Aucun algorithme n'est utilisé pour reconnaître des schémas ou effectuer des corrélations automatiques; la proportionnalité juridique et la traçabilité des décisions sont centrales.

Deux fois par an, la DPC effectue des contrôles des journaux de requêtes. En 2024, quatre avertissements ont été émis pour critères de recherche trop larges; aucune infraction grave n'a été constatée. Le rapport ISBAR 2024 mentionne un temps de réponse moyen de 77 secondes, sans accès non justifié et sans fuite de données.

Concernant la collaboration entre le registre ISBAR et le secteur bancaire, l'intervenant précise que chaque banque dispose d'un agent appelé *ISBAR Compliance Officer*, qui est chargé de télécharger les données en temps utile et de les communiquer correctement. En cas de non-respect de cette obligation, des amendes allant jusqu'à 250.000 euros peuvent être imposées et un signalement peut être envoyé à la Banque centrale d'Irlande.

Une concertation avec les banques a lieu régulièrement, par l'intermédiaire de la *Banking and Payments Federation of Ireland* (BPF). Cette concertation porte notamment sur les normes techniques et sur l'implémentation de l'ISBAR XML Schema 2.1, qui est appliqué par tous les établissements. Les mises à jour sont effectuées par l'intermédiaire d'API sous protocole TLS 1.3. Depuis 2024, le soutien des fournisseurs de monnaie électronique est également obligatoire.

Le modèle irlandais favorise la co-régulation: le secteur privé fournit des données précises tandis que l'État assure l'accès et la protection de la vie privée. Cela débouche sur un taux de conformité particulièrement élevé de 99,9 %.

Ierland is onderworpen aan de evaluaties van de *Financial Action Task Force* (FATF), waarbij het land als grotendeels conform werd geclassificeerd voor aanbeveling 29 betreffende rekeningregisters. De Europese Commissie heeft de duidelijke juridische kaders en de hoge operationele efficiëntie zonder algoritmische profilering benadrukt.

Het systeem verwerkt jaarlijks ongeveer 10,8 miljoen actieve records. In 2024 werden dagelijks 47.000 records opgeladen, met een gemiddelde responstijd van 34 seconden en een foutenmarge van 0,05 %. Er werd geen onrechtmatige toegang vastgesteld.

Kwalitatieve resultaten tonen aan dat het systeem een snellere identificatie van rekeninghouders en witwaszaken mogelijk maakt. De spreker merkt op dat recentelijk in de pers gemeld werd dat het gerecht 23 miljoen euro aan crypto in beslag heeft genomen. Op een bepaald moment werd een USB-sleutel aangetroffen in een woning, maar de verwerking hiervan duurde weken. Op de USB-sleutel stonden codes voor identificatie van cryptoactiva, maar in de tussentijd wisten de verdachten de rekeningen leeg te maken.

De heer Van Quickenborne benadrukt dat dit voorbeeld illustreert dat efficiëntere werkwijzen soms belangrijker zijn dan extra personele middelen. Hij wijst erop dat structureel al 600 miljoen euro extra in justitie is geïnvesteerd. Hij stelt dat fouten, zoals vertragingen bij het openen van beslagen of verkeerde toewijzing aan rechtbanken, ook met organisatorische verbeteringen kunnen worden beperkt.

Vervolgens keert hij terug naar de evaluatie van het ISBAR-systeem in Ierland. Een belangrijk kwalitatief resultaat is de verbeterde coördinatie tussen de Ierse financiële inlichtingeneenheid, de Ierse belastingdienst en de politie. Deze coördinatie draagt bij aan een hoger publiek vertrouwen, mede dankzij de volledige naleving van de AVG-regelgeving.

De heer Van Quickenborne bespreekt vervolgens de beperkingen van het Ierse ISBAR-systeem. Ten eerste bestaat er geen realtime connectie met de banken. Hij vraagt de minister naar de situatie in België: bestaat er met het CAP-systeem een realtime connectie met de banken?

Ten tweede wijst hij op de afhankelijkheid van handmatige validatie bij internationale verzoeken, hetgeen de verwerking vertraagt. Hij vraagt de minister naar mogelijke verbeteringen en beleidsinitiatieven.

L'Irlande est soumise aux évaluations du Groupe d'action financière (GAFI), le pays ayant été jugé en grande partie conforme à la recommandation 29 portant sur les registres de comptes. La Commission européenne a salué la clarté des cadres juridiques et la grande efficacité opérationnelle d'un système qui ne recourt pas au profilage algorithmique.

Le système traite annuellement environ 10,8 millions d'enregistrements actifs. En 2024, quelque 47.000 enregistrements ont été téléchargés quotidiennement, avec un temps de réponse moyen de 34 secondes et une marge d'erreur de 0,05 %. Aucun accès irrégulier n'a été constaté.

Les résultats qualitatifs démontrent que le système permet une identification plus rapide des titulaires de compte et des faits de blanchiment. L'intervenant fait observer que la presse a récemment fait état de la saisie par la justice de 23 millions d'euros en crypto-monnaie. À un certain moment, une clef USB a été retrouvée dans une habitation, mais le traitement des données qu'elle contenait a duré des semaines. La clef contenait des codes d'identification de crypto-actifs, mais, dans l'intervalle, les suspects avaient vidé les comptes.

M. Van Quickenborne souligne que cet exemple illustre qu'il est parfois plus important d'adopter des méthodes de travail plus efficaces que de recruter plus de personnel. Il indique que, structurellement, 600 millions d'euros supplémentaires ont déjà été investis dans la justice. Il indique que certains dysfonctionnements, comme des retards lors de l'ouverture de saisies ou l'attribution erronée de dossiers à des tribunaux, peuvent également être limités à l'aide d'améliorations organisationnelles.

Ensuite, l'intervenant revient sur l'évaluation du système ISBAR en Irlande. L'amélioration de la coordination entre l'unité d'information financière irlandaise, l'administration fiscale irlandaise et la police est un résultat important en termes de qualité du système. Cette coordination contribue à accroître la confiance de la population, notamment grâce à un respect strict du RGPD.

M. Van Quickenborne aborde ensuite les limites du système irlandais ISBAR. Tout d'abord, il n'y a pas de connexion en temps réel avec les banques. Il interroge le ministre quant à la situation en Belgique: le système PCC permet-il une connexion en temps réel avec les banques?

Ensuite, il évoque la validation manuelle des demandes internationales, qui ralentit dès lors le traitement. Il demande au ministre si des améliorations ou des initiatives sont prévues en la matière.

De heer Van Quickenborne noemt enkele voorgestelde maatregelen: de invoering van snellere API's zonder centrale datarePLICatie, de ontwikkeling van privacybeschermende analyse voor geanonimiseerde statistiek en verdere automatisering van het toezicht van de DPC met realtime meldingen.

Hij benadrukt dat het Ierse model bewijst dat efficiëntie en privacy geen tegenpolen zijn. Door het strikte verbod op datamining behoudt het register publiek vertrouwen en juridische robuustheid. Samen met Duitsland, Oostenrijk en Luxemburg behoort Ierland tot het zogenaamde *privacy-first interoperability model*. Zwitserland maakt hier geen deel van uit.

Daarnaast verwijst hij naar geplande hervormingen in Ierland in 2026, de zogenaamde *ISBAR Reform Bill*. De hervormingen omvatten realtime validatie zonder dataopslag, formele integratie met het UBO-register en extra middelen voor het toezicht door de DPC.

Het ISBAR is een voorbeeld van technologische precisie binnen een sterk juridisch kader. Het systeem combineert operationele efficiëntie met de bescherming van persoonlijke gegevens en wordt beschouwd als een van de meest evenwichtige modellen in Europa. De kernpunten ervan zijn dagelijkse dataversing met minimale fouten, geen datamining, geen profilering, volledige naleving van EU-richtlijnen en strikt toezicht door de DPC.

De spreker meent dat het ISBAR sinds de oprichting in 2021 heeft bewezen dat effectieve witwasbestrijding en bescherming van burgerrechten perfect combineerbaar zijn. Het systeem ondersteunt zowel criminaliteitsbestrijding als bescherming van de fundamentele rechten van de burger.

De heer Van Quickenborne bespreekt vervolgens de effectiviteit van het Ierse ISBAR-systeem en vergelijkt het met andere modellen, met bijzondere aandacht voor de sterktes en structurele uitdagingen.

Ten eerste behandelt hij de operationele prestaties. ISBAR presteert uitstekend op het vlak van snelheid, betrouwbaarheid en consistentie, met een beschikbaarheid van 99,97 % uptime. Volgens cijfers van de Europese Commissie behoort ISBAR tot de meest efficiënte AML-instrumenten binnen de Europese Unie. De financiële inlichtingeneenheid van Ierland meldt dat in 42 % van de witwasonderzoeken ISBAR een rol speelde bij de

M. Van Quickenborne mentionne plusieurs mesures proposées: l'introduction d'API plus rapides sans réPLication centrale des données, le développement d'analyses protégeant la vie privée à des fins de statistiques anonymisées et le renforcement de l'automatisation de la surveillance de la DPC avec des notifications en temps réel.

Il souligne que le modèle irlandais prouve qu'efficience et protection de la vie privée ne sont pas incompatibles. Grâce à l'interdiction stricte du *data mining*, le registre conserve la confiance du public et sa solidité juridique. Comme l'Allemagne, l'Autriche et le Luxembourg, l'Irlande a opté pour un modèle d'interopérabilité donnant priorité au respect de la vie privée (*privacy-first interoperability model*). La Suisse ne compte pas parmi ces pays.

L'intervenant renvoie aussi aux réformes que l'Irlande prévoit de mener en 2026 dans le cadre de la loi *ISBAR Reform Bill*. Ces réformes prévoient la validation en temps réel sans stockage de données, une intégration formelle avec le registre UBO et des moyens supplémentaires pour la surveillance par la DPC.

L'ISBAR est un exemple d'outil de précision technologique soumis à un cadre juridique solide. Le système combine efficacité opérationnelle et protection des données personnelles, et il est considéré comme l'un des modèles les plus équilibrés d'Europe. Ses éléments fondamentaux sont la mise à jour quotidienne des données avec un minimum d'erreurs, l'absence de *data mining*, l'absence de profilage, le respect total des directives européennes et une surveillance stricte par la DPC.

L'intervenant estime que, depuis sa création en 2021, l'ISBAR a prouvé qu'il était parfaitement possible de combiner efficacement la lutte contre le blanchiment d'argent et la protection des droits des citoyens. Le système soutient à la fois la lutte contre la criminalité et la protection des droits fondamentaux des citoyens.

M. Van Quickenborne aborde ensuite l'efficacité du système irlandais ISBAR et le compare à d'autres modèles, en accordant une attention particulière à ses points forts et aux défis structurels avec lesquels il doit composer.

Il évoque d'abord les prestations opérationnelles. L'ISBAR enregistre d'excellentes prestations sur le plan de la rapidité, de la fiabilité et de la cohérence, avec un temps de bon fonctionnement de 99,97 %. Selon les chiffres de la Commission européenne, l'ISBAR fait partie des outils de lutte contre le blanchiment les plus efficaces au sein de l'Union européenne. La cellule de renseignement financier irlandaise indique que, dans

eerste identificatie van verdachte rekeningen. De heer Van Quickenborne vraagt de minister naar de vergelijkbare situatie in België.

Vervolgens bespreekt hij de efficiëntie in de rechts-handhaving. Voor de invoering van ISBAR konden de politie en de financiële inlichtingeneenheid weken verliezen bij het verzamelen van informatie van rekeningen. Sinds de invoering van ISBAR is de gemiddelde reactietijd tussen het verzoek en het resultaat gedaald van tien dagen naar enkele minuten. Dit maakt het voor de *Criminal Assets Bureau* van Ierland mogelijk het criminele vermogen effectief te traceren.

De heer Van Quickenborne wijst erop dat bij de integratie van nieuwe financiële instrumenten, zoals crypto, efficiëntie cruciaal blijft. Indien de Belgische justitie niet over de vereiste middelen beschikt om dergelijke activa snel te traceren, kan dit leiden tot vermogensverlies. Hij benadrukt dat extra financiële middelen niet automatisch leiden tot betere resultaten als de organisatorische en technische capaciteit ontbreekt.

Ten slotte bespreekt het lid de kostenefficiëntie. De operationele kost van ISBAR wordt geschat op 3,2 miljoen euro, terwijl de voordelen in termen van sneller onderzoek, lagere administratieve lasten en verminderde fraude aanzienlijk hoger worden ingeschat, tot ongeveer 25 miljoen euro. De spreker maakt een kritische kanttekening bij de socialistische aanpak om eerst middelen te verhogen om vervolgens meer opbrengsten te genereren, gelet op het hoge percentage aan overheidsuitgaven in België.

De heer Van Quickenborne zou van de minister willen vernemen of het CAP het vermogen van de snelheid van vermogensbevrozing al dan niet verhoogd heeft. Daarnaast wijst hij op de baten van 25 miljoen euro tegenover de kosten van 3,2 miljoen euro en vraagt hoe deze verdeling in België is vormgegeven. Zijn hierover berekeningen uitgevoerd?

Inzake de maatschappelijke legitimiteit, verwijst de heer Van Quickenborne naar de steun van 76 % van de Ierse bevolking voor ISBAR en stelt dat dit grotendeels te danken is aan de transparante rapportage door de Ierse belastingdienst en het toezicht van de DPC.

Vervolgens situeert de spreker Ierland binnen de EU-modellen. In de Unie bestaan drie typen systemen:

42 % des enquêtes sur le blanchiment d'argent, l'ISBAR a joué un rôle dans l'identification initiale des comptes suspects. M. Van Quickenborne demande au ministre ce qu'il en est en Belgique.

Il aborde ensuite l'efficacité en matière d'application de la loi. Avant la mise en place d'ISBAR, la police et la cellule de renseignement financier pouvaient perdre des semaines à collecter des informations sur des comptes. Depuis la mise en place d'ISBAR, le délai moyen entre la demande et le résultat est passé de dix jours à quelques minutes. Cela permet au Bureau irlandais des capitaux criminels (*Criminal Assets Bureau*) de retracer efficacement les avoirs criminels.

M. Van Quickenborne souligne que l'efficacité reste cruciale lors de l'intégration de nouveaux instruments financiers, comme les cryptomonnaies. Si la justice belge ne dispose pas des moyens nécessaires pour retracer rapidement ces actifs, cela peut entraîner une perte patrimoniale. Il insiste sur le fait que des moyens financiers supplémentaires n'entraînent pas automatiquement des meilleurs résultats si les capacités organisationnelles et techniques font défaut.

Enfin, le membre aborde la question du rapport coût-efficacité. Le coût opérationnel de l'ISBAR est estimé à 3,2 millions d'euros, tandis que les gains qu'il génère en matière d'accélération des enquêtes, de réduction de la charge administrative et de diminution de la fraude sont estimés à un montant nettement supérieur (jusqu'à environ 25 millions d'euros). L'intervenant fustige l'approche socialiste consistant à augmenter d'abord les moyens pour ensuite générer davantage de recettes, compte tenu du pourcentage élevé des dépenses publiques en Belgique.

M. Van Quickenborne demande au ministre si le PCC a permis ou non d'accélérer le gel des avoirs. Le membre souligne en outre le rapport coût-efficacité du système irlandais (un gain de 25 millions d'euros pour un coût de 3,2 millions d'euros). Il demande quel est le rapport coût-efficacité du système belge. Des calculs ont-ils été effectués à ce sujet?

En ce qui concerne la légitimité sociale, M. Van Quickenborne renvoie au fait que 76 % de la population irlandaise soutient l'ISBAR et indique que ce large soutien est en grande partie dû à la transparence du rapportage publié par l'administration fiscale irlandaise et au contrôle exercé par la DPC.

L'intervenant précise ensuite dans quelle catégorie se classe l'Irlande parmi les systèmes existant au sein

centrale registers met analysecapaciteit, gedecentraliseerde querysystemen en hybride identificatiemodellen.

Ten eerste de centrale registers, zoals in België, Frankrijk en Spanje. Voor de duidelijkheid licht hij toe dat Frankrijk en Spanje in deze bespreking niet verder aan bod komen, omdat deze systemen vergelijkbaar zijn met België.

Ten tweede de gedecentraliseerde querysystemen, zoals in Duitsland, Oostenrijk en Nederland.

Ten derde de hybride identificatiemodellen, waaronder Ierland en Luxemburg ressorteren. Deze modellen combineren centrale opslag met een verbod op datamining, waardoor de voordelen van centralisatie worden gecombineerd met de privacybescherming van het decentrale model.

De heer Van Quickenborne merkt op dat in België de beheerder de Nationale Bank is, terwijl in Ierland de toegang tot het systeem beperkt is en datamining verboden blijft. Het publieke draagvlak in Ierland is hoog, terwijl dit in België gematigd is.

Hoewel de analysetools in België krachtiger zijn dan in Ierland, scoort Ierland beter op het vlak van zekerheid, vertrouwen en transparantie.

De vergelijking met Duitsland en Oostenrijk toont dat beide landen querymodellen hanteren zonder centrale opslag. Ierland biedt meer snelheid dankzij de gecentraliseerde database, maar met vergelijkbare privacygaranties. In alle drie de gevallen geldt een verbod op datamining en automatische analyses.

Sterktes van het Ierse model

De heer van Quickenborne vat de sterktes van het Ierse model samen. Allereerst is er de juridische helderheid van het model, het feit dat het doel en de toegang zijn gedefinieerd. Het verbod op datamining is grondwettelijk verankerd. Ook de technische betrouwbaarheid vormt een sterkte van het Ierse model. Het systeem is uitzonderlijk stabiel, kent geen storingen of datalekken en voldoet aan twee ISO-normen.

Voorts gaat de spreker in op de *governance* en *accountability* van het Ierse systeem. Het beheer wordt waargenomen door de *Revenue*, terwijl het toezicht wordt

de l'Union européenne. Il existe en effet trois types de systèmes dans l'Union: les registres centraux dotés d'une capacité d'analyse, les systèmes de requête décentralisés et les modèles d'identification hybrides.

La première catégorie est celle des registres centraux, comme en Belgique, en France et en Espagne. Par souci de clarté, il précise qu'il n'abordera pas les cas de la France et de l'Espagne dans son intervention, étant donné que leur système est comparable à celui de la Belgique.

La deuxième catégorie concerne les systèmes de requête décentralisés, comme en Allemagne, en Autriche et aux Pays-Bas.

La troisième catégorie, dont font partie l'Irlande et le Luxembourg, regroupe les modèles d'identification hybrides. Ces modèles conjuguent stockage centralisé et interdiction du *data mining*, ce qui permet de combiner les avantages de la centralisation avec la protection de la vie privée offerte par le modèle décentralisé.

M. Van Quickenborne fait observer qu'en Belgique, le gestionnaire du système est la Banque nationale, tandis qu'en Irlande, l'accès au système est limité et le *data mining* reste interdit. Le soutien de l'opinion publique est élevé en Irlande, alors qu'il est modéré en Belgique.

Bien que les outils d'analyse soient plus puissants en Belgique qu'en Irlande, cette dernière obtient de meilleurs résultats en matière de sécurité, de confiance et de transparence.

La comparaison avec l'Allemagne et l'Autriche montre que ces deux pays utilisent des modèles de requête sans stockage centralisé. L'Irlande peut agir plus rapidement grâce à sa base de données centralisée, tout en offrant des garanties comparables de respect de la vie privée. Dans les trois cas, le *data mining* et les analyses automatiques sont interdits.

Points forts du modèle irlandais

M. Van Quickenborne résume les points forts du modèle irlandais. Tout d'abord, il évoque la clarté juridique du modèle, le fait que l'objectif et l'accès soient définis. L'interdiction du *data mining* est inscrite dans la Constitution. La fiabilité technique constitue également un point fort de ce modèle. Le système est exceptionnellement stable, ne connaît pas de dysfonctionnements ni de fuites de données et satisfait à deux normes ISO.

L'intervenant aborde ensuite la gouvernance et la responsabilité dans le système irlandais. La gestion est assurée par le *Revenue*, tandis que la surveillance est

uitgeoefend door de *Data Protection Commission* (DPC), hetgeen volgens de spreker zorgt voor duidelijke *checks and balances*. Een dergelijke gestructureerde verdeling van verantwoordelijkheden ontbreekt in ons land.

De spreker wijst erop dat in Ierland diverse rapporten publiek beschikbaar zijn en dat de query-processen onafhankelijk worden geaudit. Het is niet duidelijk of dit in België ook wordt gedaan. In dat verband verwijst de heer Van Quickenborne naar het *Implementation Report 2024* van de Europese Commissie, waarin Ierland als *exemplary* wordt bestempeld met betrekking tot het bereiken van een evenwicht tussen doeltreffendheid, sociale proportionaliteit en de waarborging van grondrechten.

Daarnaast heeft de *Financial Action Task Force* (FATF) in 2023 het Ierse model geprezen voor de strikte naleving van fundamentele rechten. Ook opvallend is dat in Ierland alle politieke partijen in het nationale parlement de ISBAR-architectuur unaniem ondersteunen, inclusief Sinn Féin. Het Ierse parlement onderzoekt overigens verdere optimalisatiemogelijkheden, waarvan de spreker de uitkomst met belangstelling tegemoetziet.

Zwaktes van het Ierse model

Het lid gaat vervolgens over tot de zwaktes en structurele uitdagingen van het Ierse systeem. Een eerste zwakte betreft het ontbreken van real-time toegang. Hierdoor worden updates niet in real time beschikbaar gesteld. In dringende dossiers — zoals urgente witwas- of terrorismeonderzoeken — kan een vertraging van enkele uren een doorslaggevende hinderpaal vormen. Een hervorming naar real-time updates van het Ierse systeem, met behoud van logging en onder toezicht van de *Data Protection Commission*, wordt momenteel onderzocht. Een bijkomend nadeel is dat het grondwettelijke verbod op datamining de vroegtijdige detectie van systemische risico's kan belemmeren.

Een tweede zwakte betreft de beperkte analysecapaciteit.

Een derde uitdaging heeft betrekking op de fragmentatie van bevoegdheden. Vier instanties — de *Revenue*, de DPC, de Central Bank en de CFI — beschikken elk over afzonderlijke mandaten. Het ontbreken van een nationale coördinatieraad leidt ertoe dat samenwerking soms wordt vertraagd.

Een vierde aandachtspunt betreft de toenemende Europese harmonisatiedruk. De toekomstige *Anti-Money Laundering Authority* (AMLA) zal naar verwachting een uniform standaardmodel opleggen. De uitdaging voor

exercée par la *Data Protection Commission* (DPC), ce qui, selon l'intervenant, garantit un équilibre clair des pouvoirs. Cette répartition structurée des responsabilités fait défaut dans notre pays.

L'intervenant souligne qu'en Irlande, un certain nombre de rapports sont accessibles au public et que les processus de requête font l'objet d'un audit indépendant. Il n'apparaît pas clairement si c'est également le cas en Belgique. À cet égard, M. Van Quickenborne renvoie au rapport de mise en œuvre publié par la Commission européenne en 2024, dans lequel l'Irlande est qualifiée d'exemplaire en ce qui concerne l'équilibre entre efficacité, proportionnalité sociale et garantie des droits fondamentaux.

Par ailleurs, en 2023, le Groupe d'action financière (GAFI) a salué le modèle irlandais pour son strict respect des droits fondamentaux. Il est également frappant de constater qu'en Irlande, tous les partis politiques représentés au Parlement national, y compris le Sinn Féin, soutiennent à l'unanimité l'architecture ISBAR. Le Parlement irlandais examine d'ailleurs d'autres possibilités d'optimisation, dont l'intervenant attend les résultats avec intérêt.

Faiblesses du modèle irlandais

Le membre évoque ensuite les faiblesses et les défis structurels du système irlandais. Une première faiblesse est l'absence d'accès en temps réel. De ce fait, les mises à jour ne sont pas disponibles en temps réel. Dans les dossiers urgents, comme certaines enquêtes sur le blanchiment d'argent ou le terrorisme, un retard de quelques heures peut constituer un obstacle décisif. L'Irlande envisage une réforme visant à mettre en place des mises à jour en temps réel du système, tout en conservant le *logging*, sous le contrôle de la *Data Protection Commission*. Un inconvénient supplémentaire est que l'interdiction constitutionnelle du *data mining* peut entraver la détection précoce de risques systémiques.

Une deuxième faiblesse est la capacité d'analyse limitée.

Un troisième défi concerne la fragmentation des compétences. Quatre instances — le *Revenue*, la DPC, la *Central Bank* et la CTIF — disposent chacune de mandats distincts. L'absence d'un conseil national de coordination entraîne parfois des retards dans la coopération.

Le quatrième point sur lequel le membre attire l'attention est la pression croissante exercée par l'harmonisation européenne. La future Autorité de lutte contre le blanchiment de capitaux (ALBC) devrait imposer un modèle

Ierland zal erin bestaan zijn privacy-firstbenadering te behouden binnen dit Europese kader, een opdracht die volgens de spreker zal toekomen aan de opvolger van minister Paschal Donohoe.

Ierland behoort tot de zogeheten conservatief-liberale staten binnen de AMLA-architectuur, die prioriteit geven aan privacy en proportioneel toezicht. Binnen de AMLA-werkgroep, waarin België eveneens zetelt, neemt Ierland het voortouw in het debat over data-ethiek en proportionaliteit.

Ierland vormt daarnaast een belangrijk financieel knooppunt voor tal van internationale instellingen: meer dan vierduizend beleggingsfondsen en meer dan negentig banken zijn er actief. De ISBAR-infrastructuur versterkt, aldus de heer Van Quickenborne, de reputatie van Dublin als een transparante, doch rechtszekere financiële hub.

Bovendien merkt hij op dat de Ierse benadering ook een invloed uitoefent op wetgeving in andere lidstaten. Zo hebben Malta en Cyprus hun systemen mede op het Ierse model gebaseerd en eveneens een dataminingsverbod ingevoerd.

Een tussentijdse conclusie over het Ierse model is dat het een functioneel, efficiënt en ethisch model is, dat technologische robuustheid combineert met juridische proportionaliteit. De grootste uitdaging ervan ligt niet zozeer in de werking ervan, maar wel in het bewaren van zijn autonomie binnen de AMLA structuur. Het Ierse model bewijst dat men innovatieve manieren van werken kan combineren met de privacy-firstbenadering. Ierland bewijst op deze manier dat financiële integriteit en burgerlijke vrijheid geen tegenstaande krachten hoeven te zijn. In het Ierse systeem zijn ze mooi in balans.

Prioriteiten voor de toekomst

In de strategische review van het Ierse systeem worden een aantal kernprioriteiten voor de toekomst geformuleerd. Ook daar heeft Ierland een voorsprong op België. Het lijkt er immers op dat de Belgische minister van Financiën helemaal geen doelstellingen voor de toekomst heeft voor wat het CAP betreft.

De kernprioriteiten voor de toekomst zijn als volgt:

De verhoging van de efficiëntie, technologische modernisering en een verbeterde gegevensstroom. Daarnaast zal er worden geijverd voor het versterken van het toezicht en de verantwoording, via een permanente coördinatie-structuur en uitgebreide rapportage. Een laatste prioriteit

standard uniforme. Le défi pour l'Irlande consistera à conserver son approche axée sur la protection de la vie privée dans le cadre de cet environnement européen, une tâche qui, selon l'intervenant, reviendra au successeur du ministre Paschal Donohoe.

Au sein de l'architecture ALBC, l'Irlande fait partie des États dits conservateurs-libéraux, qui accordent la priorité à la vie privée et à une surveillance proportionnée. Au sein du groupe de travail ALBC, dont la Belgique fait également partie, l'Irlande prend la tête du débat sur l'éthique des données et la proportionnalité.

L'Irlande constitue en outre un centre financier important pour de nombreuses institutions internationales: plus de quatre mille fonds d'investissement et plus de nonante banques y sont actifs. Selon M. Van Quickenborne, l'infrastructure ISBAR renforce la réputation de Dublin en tant que centre financier transparent offrant malgré tout une sécurité juridique.

Par ailleurs, le membre fait observer que l'approche irlandaise influence aussi la législation d'autres États membres. Ainsi, Malte et Chypre ont en partie basé leurs systèmes sur le modèle irlandais et ont également introduit une interdiction du *data mining*.

Une conclusion intermédiaire concernant le modèle irlandais est qu'il s'agit d'un modèle fonctionnel, efficace et éthique, qui allie robustesse technologique et proportionnalité juridique. Le principal défi ne réside pas tant dans son fonctionnement que dans le maintien de son autonomie au sein de la structure ALBC. Le modèle irlandais démontre qu'il est possible de combiner des procédés innovants avec une approche privilégiant la protection de la vie privée. L'Irlande démontre ainsi que l'intégrité financière et les libertés civiles ne sont pas nécessairement incompatibles. Dans le système irlandais, elles sont en parfait équilibre.

Priorités pour l'avenir

La revue stratégique du système irlandais est l'occasion de formuler un certain nombre de priorités clés pour l'avenir. Là encore, l'Irlande a une longueur d'avance sur la Belgique. Il semble en effet que le ministre belge des Finances n'ait aucun objectif pour l'avenir en ce qui concerne le PCC.

Les priorités clés pour l'avenir sont les suivantes:

l'augmentation de l'efficacité, la modernisation technologique et l'amélioration du flux de données. En outre, des efforts seront déployés pour renforcer le contrôle et la responsabilité, grâce à une structure de coordination permanente et à un élargissement du rapportage. Une

is het behouden van de proportionaliteit. Zijn er voor het Belgische CAP ook beleidsdoelstellingen? En zo ja, waaruit bestaan die dan? Wat wenst de minister te doen op het vlak van efficiëntie? Wat wenst hij te doen op het vlak van toezicht en verantwoording en op het vlak van proportionaliteit?

Naast de doelstellingen voor de komende jaren, beschikt Ierland over een aantal fundamentele principes die richting geven aan het beleid. Dat zijn *legal certainty*, *data minimisation* en *transparent governance*.

De heer Van Quickenborne legt uit wat deze principes inhouden. Hij verwijst vooreerst naar het principe van de *legal certainty*, of de rechtszekerheid. Elke verwerking van persoonsgegevens moet gebaseerd zijn op een uitdrukkelijke wettelijke grondslag. Bovendien mag uitsluitend informatie worden bijgehouden die strikt noodzakelijk is voor het beoogde doel. Hij werpt daarbij de vraag op of het opslaan van alle bankrekeningen en alle saldi van 11 miljoen Belgen nog als proportioneel kan worden beschouwd. Is dit werkelijk de noodzakelijke informatie die moet worden verzameld, ook van burgers die bijvoorbeeld slechts 3000 euro op hun rekening hebben staan en dus hoogstens in aanmerking zouden kunnen komen voor zeer kleinschalige vormen van fraude?

Vervolgens gaat hij in op het principe van *transparent governance*. Elke raadpleging en elke wijziging moet traceerbaar en verantwoord zijn. De spreker vraagt zich af of die pijler eveneens is verankerd in het voorgestelde Belgische beleid.

Geplande wetgevende hervormingen

De heer Van Quickenborne legt vervolgens uit welke wetgevende hervormingen gepland zijn in Ierland. Ten eerste wordt er een ISBAR-wetsontwerp voorbereid door de regering. Dat zal in 2026 aan het Parlement worden voorgelegd. De belangrijkste vernieuwingen van dat wetsontwerp zullen de volgende zijn: de verankering van het dataminingsverbod in primair recht, de verplichte rapportage van alle ISBAR-statistieken aan het parlement, de verduidelijking van de sancties bij overtreding en de formele verankering van het DPC-toezicht in de wet. Wat voorziet de Belgische minister van Financiën om de werking van het CAP te verbeteren?

Een andere wetgevende hervorming zal betrekking hebben op de realtime-queryoptie. Men zal ervoor zorgen dat voor uitzonderlijke situaties in een realtime *access protocol* wordt voorzien. Voorziet de minister ook in realtime *queries* voor het CAP?

dernière priorité est le maintien de la proportionnalité. Existe-t-il également des objectifs politiques pour le PCC belge? Si oui, quels sont-ils? Que souhaite faire le ministre en matière d'efficacité? Quels sont ses objectifs en matière de contrôle, de responsabilité et de proportionnalité?

Outre les objectifs fixés pour les années à venir, l'Irlande dispose d'un certain nombre de principes fondamentaux qui orientent sa politique. Il s'agit de la sécurité juridique, de la minimisation des données et de la transparence de la gouvernance.

M. Van Quickenborne explique ce qu'impliquent ces principes. Il fait tout d'abord référence au principe de la sécurité juridique (*legal certainty*). Tout traitement de données à caractère personnel doit reposer sur une base légale explicite. De plus, seules les informations strictement nécessaires à l'objectif poursuivi peuvent être conservées. À cet égard, il soulève la question de savoir si le stockage de tous les comptes bancaires et de tous les soldes de 11 millions de Belges peut encore être considéré comme proportionné. S'agit-il vraiment des informations qui doivent nécessairement être collectées? Qu'en est-il des informations relatives aux citoyens qui, par exemple, n'ont que 3.000 euros sur leur compte et ne pourraient donc être concernés que par des formes de fraude à très petite échelle?

Il aborde ensuite le principe de la transparence de la gouvernance (*transparent governance*). Chaque consultation et chaque modification doivent être traçables et justifiées. L'intervenant se demande si ce pilier est également intégré à la politique belge proposée.

Réformes législatives prévues

M. Van Quickenborne explique ensuite quelles réformes législatives sont prévues en Irlande. Tout d'abord, le gouvernement est en train de préparer un projet de loi ISBAR, qui sera soumis au Parlement en 2026. Les principales innovations de ce projet de loi seront les suivantes: l'ancrage de l'interdiction du *data mining* dans le droit primaire, l'obligation de procéder au rapportage de toutes les statistiques relatives à l'ISBAR au Parlement, la clarification des sanctions en cas d'infraction et l'ancrage formel du contrôle de la DPC dans la loi. Que prévoit le ministre des Finances belge pour améliorer le fonctionnement du PCC?

Une autre réforme législative concernera l'option de requête en temps réel. Un protocole d'accès en temps réel sera prévu dans des situations exceptionnelles. Le ministre prévoit-il également des requêtes en temps réel pour le PCC?

Een derde wetgevende hervorming is de integratie met het *Register of Beneficial Ownership*. Het Ierse ministerie van Financiën onderzoekt een gecontroleerde koppeling tussen ISBAR en het *Register of Beneficial Ownership*, het Ierse equivalent van het Belgische UBO-register. Die koppeling zal uitsluitend gebeuren via het systeem van pseudonymisering, zodat de identiteit van de uiteindelijke eigenaar enkel zichtbaar zal zijn voor de bevoegde instanties met gerechtelijke machtiging. Hoe zit dat in België? Hoe zit het met de integratie van het CAP en het UBO-register? Is dat bij ons ook voorzien? Zal er ook met pseudonymisering worden gewerkt?

De vierde wetgevende hervorming zal de versterking van de toezichtstructuur zijn. Er komt een, *National Transparency Board* (NTB), een multidisciplinair orgaan, met vertegenwoordigers van onder andere de *Revenue*, de DPC, de Politie, de *Central Bank*, en de Ierse Bankenfederatie. Dat NTB zal beleidsadvies geven, zal audits coördineren en zal een nationale rapportage richting de AMLA verzorgen. Wordt in België een versterking van de toezichtstructuur gepland?

Technologische en organisatorische vernieuwingen

Vervolgens gaat de heer Van Quickenborne in op de technologische en organisatorische vernieuwingen die in Ierland worden voorbereid. Ten eerste zal de *Revenue* in 2026 de infrastructuur upgraden. Ze zal de database van de ISBAR migreren naar een *container-based cloud*-omgeving met *zero-trust security architecture*. Men wil op die manier de flexibiliteit verhogen en de operationele kosten verlagen. Hoe verhoudt de Belgische CAP zich ten opzichte van zo'n plan?

Er zal vervolgens worden ingezet op *privacy-preserving analytics*. Dat zijn technologieën die toelaten om statistische inzichten te verwerven zonder dat individuele persoonsgegevens moeten worden verwerkt. Het doel is om beleidsinformatie te genereren zonder dat men het dataminingsverbod doorbreekt. Zal de Belgische minister ook gebruikmaken van *privacy preserving analytics*?

Ierland zal ook overgaan tot de automatisering van het DPC-toezicht. Men zal een *supervised logging interface* ontwikkelen waarbij men in real-time waarschuwingen ontvangt bij onregelmatigheden. Zal hierin worden voorzien in het Belgische systeem?

Een vierde technologische en organisatorische vernieuwing die in Ierland wordt gepland, is het jaarlijks verplichten van gebruikers om een *ISBAR ethics and data protection training* te volgen. De gebruikers zullen

Une troisième réforme législative concerne l'intégration avec le *Register of Beneficial Ownership*. Le ministère irlandais des Finances examine actuellement la possibilité d'établir un couplage contrôlé entre l'ISBAR et le *Register of Beneficial Ownership*, l'équivalent irlandais du registre UBO belge. Ce couplage sera établi exclusivement via le système de pseudonymisation, de sorte que l'identité du propriétaire ultime ne sera visible que pour les autorités compétentes disposant d'une habilitation judiciaire. Qu'en est-il en Belgique? Qu'en est-il d'une intégration du PCC avec le registre UBO? Est-ce également prévu chez nous? La pseudonymisation sera-t-elle également utilisée?

La quatrième réforme législative portera sur le renforcement de la structure de contrôle. Un organe pluridisciplinaire, le *National Transparency Board* (NTB), sera créé. Il rassemblera notamment des représentants du *Revenue*, de la DPC, de la police, de la *Central Bank* et de la Fédération bancaire irlandaise. Le NTB fournira des conseils politiques, coordonnera les audits et établira un rapportage national à l'intention de l'ALBC. Un renforcement de la structure de contrôle est-il prévu en Belgique?

Innovations technologiques et organisationnelles

M. Van Quickenborne aborde ensuite les innovations technologiques et organisationnelles prévues en Irlande. Tout d'abord, le *Revenue* modernisera son infrastructure en 2026. Il migrera la base de données de l'ISBAR vers un environnement *cloud* structuré en conteneurs et selon un modèle à vérification systématique. L'objectif est d'accroître la flexibilité et de réduire les coûts opérationnels. Comment le PCC belge se positionne-t-il par rapport à un tel projet?

Le *Revenue* mettra ensuite sur les techniques d'analyse respectueuses de la vie privée (*privacy analytics*). Il s'agit de technologies qui permettent d'obtenir des informations statistiques sans devoir traiter de données à caractère personnel individuelles. L'objectif est de générer des informations stratégiques sans enfreindre l'interdiction du *data mining*. Le ministre belge aura-t-il également recours à ces techniques d'analyse?

L'Irlande entend également automatiser le contrôle exercé par la DPC. Une interface de contrôle de la journalisation sera développée afin que des alertes soient émises en temps réel en cas d'irrégularité. Cette fonctionnalité sera-t-elle intégrée au système belge?

Une quatrième innovation technologique et organisationnelle prévue en Irlande consiste à obliger les utilisateurs à suivre chaque année une formation ISBAR sur l'éthique et la protection des données. Les utilisateurs

een training krijgen over grondrechten en gegevensverwerking. Ze zullen ook lessen krijgen over informatiebeveiliging en risico-inschatting. De cursisten zullen daarnaast praktische casussen moeten oplossen. Dit alles heeft tot doel om de compliancecultuur binnen de administratie te versterken. Hoe zit het met de trainingen en competentieontwikkeling in ons land in het kader van het CAP en in het kader van de ontwikkelingen op het vlak van *money control*?

De heer Van Quickenborne besluit dit gedeelte met nog een aantal hervormingen die men in Ierland voor ogen heeft. Ten eerste zal de *Revenue* elk jaar een *ISBAR Transparency Report* publiceren dat zal worden besproken in de *Joint Committee on Finance*, waardoor de democratische controle structureel wordt. Is dat iets wat ook in de parlementaire commissie Financiën mogelijk zou zijn? Voorts zal men werken aan het onafhankelijk toezicht door de DPC. De *Data Protection Commission* zal rechtstreeks toegang krijgen tot auditlogs. De DPC zal de bevoegdheid krijgen om onmiddellijke waarschuwingen aan de minister over te maken en een mogelijkheid om sancties op te leggen tot 5 miljoen euro bij ernstige overtredingen. Belgische toezichthoudende instanties kunnen slechts sancties tot 500.000 euro opleggen. Tot slot zal er worden ingezet op externe evaluatie. In Ierland zal men om de vijf jaar een onafhankelijke academische evaluatie laten plaatsvinden. De eerste evaluatie zal in 2027 plaatsvinden. Plant België ook een dergelijke evaluatie? En zal die tweejaarlijks, driejaarlijks of meerjaarlijks worden uitgevoerd?

Internationale positionering

Hoe positioneert Ierland zich nu internationaal? Binnen de Europese Unie pleit Ierland, dat zich binnen de AMLA als *ethical transparency leader* positioneert, voor drie zaken.

Het land pleit in de eerste plaats voor één technische standaard voor interoperabiliteit. Ten tweede pleit Ierland voor een nationale autonome gegevensverwerking. Men is dus van mening dat, ondanks het feit dat men internationaal moet samenwerken, gegevens op nationaal niveau bewaard moeten blijven. Ten derde pleit Ierland systematisch voor verplichte, onafhankelijke toezichthouders.

Wat is de houding van België binnen de AMLA? Is ons land ook voortrekker? En op welke domeinen onderscheidt ons land zich van de andere landen?

recevront une formation sur les droits fondamentaux et le traitement des données. Ils suivront également des cours sur la sécurité de l'information et sur l'évaluation des risques. Les participants devront en outre résoudre des cas pratiques. Cette formation vise à renforcer la culture de la conformité au sein de l'administration irlandaise. Qu'en est-il des formations et du développement des compétences dans notre pays dans le cadre du PCC et dans le cadre des développements en matière de *money control*?

M. Van Quickenborne conclut ce volet de son analyse en évoquant une série d'autres réformes envisagées en Irlande. Tout d'abord, le *Revenue* publiera chaque année un *ISBAR Transparency Report* qui sera examiné par le *Joint Committee on Finance*, ce qui conférera une dimension structurelle au contrôle démocratique. Pourrait-on envisager un dispositif similaire en commission des Finances de la Chambre? L'Irlande entend en outre œuvrer à la mise en place d'un contrôle indépendant par la *Data Protection Commission*. Cette DPC aura un accès direct aux journaux d'audit. Elle sera habilitée à adresser des avertissements immédiats au ministre et à infliger des sanctions pouvant aller jusqu'à 5 millions d'euros en cas d'infraction grave. À titre de comparaison, les autorités de contrôle belges ne peuvent pas infliger de sanctions excédant 500.000 euros. Enfin, l'accent sera mis sur l'évaluation externe. En Irlande, une évaluation indépendante sera réalisée tous les cinq ans par des universitaires. La première évaluation aura lieu en 2027. La Belgique prévoit-elle également une telle évaluation? Dans l'affirmative, à quelle fréquence: tous les deux ans, tous les trois ans ou davantage?

Positionnement international

Quelle place l'Irlande occupe-t-elle aujourd'hui sur la scène internationale? Au sein de l'Union européenne, l'Irlande, qui se présente comme leader en matière de transparence éthique au sein de l'AMLA, défend trois points.

Elle préconise en premier lieu l'adoption d'une norme technique unique afin de favoriser l'interopérabilité. Deuxièmement, l'Irlande prône un traitement autonome des données au niveau national. Elle estime donc, en dépit de la nécessité d'une coopération internationale, que les données doivent être conservées au niveau national. Troisièmement, l'Irlande plaide systématiquement en faveur de la mise en place obligatoire de contrôleurs indépendants.

Quelle est la position de la Belgique au sein de l'AMLA? Notre pays est-il également un pionnier dans ce domaine? Et dans quels domaines la Belgique se distingue-t-elle des autres pays?

Met betrekking tot de internationale samenwerking buiten de EU, verwijst de heer Van Quickenborne naar het OESO Global Forum, waar Ierland zich profileert als voorvechter van *Human Rights Compliant AML Systems*.

Het is door deze reputatie dat Dublin internationale financiële instellingen aantrekt die belang hechten aan rechtszekerheid en vertrouwen. De spreker vreest dat, door de invoering van het systeem van *money control*, onze internationale reputatie weleens een lelijke deuk zou kunnen krijgen. België riskeert de risee te worden van de financiële wereld.

Daarom is het ook zo relevant dat de drie instellingen aan wie advies moest worden gevraagd zijn, de ECB, de Nationale Bank en de Inspectie van Financiën, niet om advies werd gevraagd. De spreker vermoedt dat die adviezen erg negatief geweest zouden zijn.

De diplomatieke en economische voordelen van de gunstige internationale positionering van Ierland mogen niet worden onderschat. Ierland is gekend als een stabiel, transparant en betrouwbaar financieel centrum. ISBAR versterkt dit gunstige imago nog. En wanneer men internationale investeerders en compliancekantoren wil aantrekken, dan heeft men een stabiel financieel kader nodig. Met de invoering van de *money control* zal België net instabiliteit creëren. De Belgische regering zal bedrijven ontmoedigen om zich in ons land te vestigen.

In België zal die *money control* overigens een belangrijk bestanddeel worden van de begroting. De regering rekent zich al rijk en meent dat de strijd tegen fiscale fraude aanzienlijke ontvangsten zal opleveren. Dat staat in schril contrast met de Ierse aanpak. Ierland voert geen *money control* in. Integendeel, Ierland rekent op terugverdieneffecten door de verlaging van de vennootschapsbelasting en een lagere btw op de horeca. Daarnaast ziet Ierland af van allerlei belastingverhogingen, die in België waarschijnlijk wel zullen worden ingevoerd.

Beleidsaanbevelingen voor België

Op basis van zijn voorstelling van het Ierse model, formuleert de heer Van Quickenborne tien beleidsaanbevelingen voor de Belgische regering.

In de eerste plaats moet België de kernprincipes van legaliteit, proportionaliteit en transparantie in de wet verankeren. Het zou nog beter zijn om deze kernprincipes grondwettelijk te verankeren. Ten tweede moet België het dataminingverbod bevestigen. Het is belangrijk dat het absolute verbod op automatische profilering en

En ce qui concerne la coopération internationale en dehors de l'Union européenne, M. Van Quickenborne renvoie au Forum mondial de l'OCDE, où l'Irlande se profile comme le défenseur des systèmes de lutte contre le blanchiment respectueux des droits humains.

C'est grâce à cette réputation que Dublin attire des institutions financières internationales qui accordent de l'importance à la sécurité juridique et à la confiance. L'orateur craint que l'introduction du système *money control* ne porte gravement atteinte à notre réputation internationale. La Belgique risque de devenir la risée du monde financier.

C'est pourquoi l'intervenant déplore vivement que les trois institutions dont l'avis aurait dû être sollicité, à savoir la BCE, la Banque nationale et l'Inspection des Finances, n'aient pas été consultées. L'orateur craint que ces avis n'aient été très négatifs.

Il ne faut pas sous-estimer les avantages diplomatiques et économiques générés par positionnement international favorable de l'Irlande. L'Irlande est connue pour être un centre financier stable, transparent et fiable. L'ISBAR renforce encore cette image favorable. Et si l'on souhaite attirer des investisseurs internationaux et des bureaux de conformité, il faut disposer d'un cadre financier stable. Avec l'introduction du *money control*, la Belgique ne créera que de l'instabilité. Le gouvernement belge dissuadera les entreprises de s'installer dans notre pays.

En Belgique, ce *money control* deviendra par ailleurs un élément important du budget. Le gouvernement se frotte déjà les mains et estime que la lutte contre la fraude fiscale générera des recettes considérables. Cette attitude contraste fortement avec l'approche irlandaise. L'Irlande n'introduit pas de *money control*. Au contraire, elle mise sur les effets retour de la réduction de l'impôt des sociétés et de la TVA dans l'horeca. En outre, l'Irlande renonce à toutes sortes d'accroissements d'impôts qui seront probablement introduits en Belgique.

Recommandations politiques pour la Belgique

Fort de sa présentation du modèle irlandais, M. Van Quickenborne formule ensuite dix recommandations politiques à l'intention du gouvernement belge.

Premièrement, la Belgique doit ancrer les principes fondamentaux de légalité, de proportionnalité et de transparence dans la loi voire, encore mieux, dans la Constitution. Deuxièmement, la Belgique doit confirmer l'interdiction du *data mining*. Il est important de maintenir l'interdiction absolue du profilage automatique et

statistische exploitatie van persoonsgegevens wordt behouden.

Ten derde moet de Belgische regering real-time toegang onder toezicht introduceren bij urgente dreigingen, zoals terrorisme en cybercrime. Vervolgens moet in België de *governance* worden versterkt. Dit doet men best door een raad te creëren, zoals de *National Transparency Board*.

Ten vijfde moet de technische weerbaarheid worden versterkt. Er moet worden gezorgd voor end-to-end-encryptie en een *zero-trust architecture*. De regering moet voorts privacy-innovatie bevorderen en aan de slag gaan met *privacy-preserving analytics*.

Een zevende werkpunt is de publieke rapportering. Er moet worden gerapporteerd over de werking van het CAP, zodat alle gebruiksstatistieken en audits publiek beschikbaar zijn.

Een achtste uitdaging is het institutionaliseren van opleidingen. Alle gebruikers zouden een jaarlijkse verplichte training moeten volgen.

Een negende aandachtspunt is het bevorderen van de Europese harmonisering, mét behoud van de nationale autonomie. De uitdaging bestaat er dus in om pro-Europees te blijven, maar de autonomie van de deelstaten te respecteren. De tiende en laatste aanbeveling is de creatie van een structurele evaluatie, oftewel een vijfjaarlijkse onafhankelijke toetsing door academische instanties.

Als deze beleidsaanbevelingen worden gevolgd,, zal het systeem robuuster en transparanter zijn en zal de rechtszekerheid in ons land worden gewaarborgd.

Strategische eindconclusies over het Ierse systeem

De heer Van Quickenborne besluit dat het Ierse model bewijst dat efficiëntie niet afhankelijk is van massale data-verwerking. Het is een model dat het vertrouwen in de mensen als een basis ziet en niet als een bijproduct. Ook is er een goed evenwicht tussen macht en gematigdheid. Het is mogelijk om financieel transparant en effectief te zijn, zonder een inbreuk op de privacy te plegen.

Voorts geeft het Ierse model een toekomstgericht perspectief. Ierland zal zijn positie als Europees referentiemodel voor ethische financiële transparantie steeds meer versterken.

de l'exploitation statistique des données à caractère personnel.

Troisièmement, le gouvernement belge doit permettre un accès contrôlé en temps réel en cas de menaces aiguës, comme le terrorisme et la cybercriminalité. Ensuite, il convient de renforcer la gouvernance en Belgique. Le meilleur moyen d'y parvenir est de créer un conseil sur le modèle du *National Transparency Board* irlandais.

La cinquième recommandation concerne le renforcement de la résilience technique. Il convient de garantir un chiffrement de bout en bout et un modèle à vérification automatique. Le gouvernement doit également promouvoir l'innovation en matière de protection de la vie privée et appliquer des techniques d'analyse respectueuses de la vie privée.

Un septième point à améliorer concerne le rapportage à l'égard du public. Il faut rendre compte du fonctionnement du PCC afin que toutes les statistiques d'utilisation et tous les audits soient accessibles au public.

Un huitième défi consiste à ancrer durablement les formations. Tous les utilisateurs du PCC devraient suivre une formation annuelle obligatoire.

La neuvième recommandation consiste à promouvoir l'harmonisation au niveau européen, tout en préservant l'autonomie nationale. L'enjeu est donc de rester pro-européen, sans porter atteinte à l'autonomie des États membres. La dixième et dernière recommandation concerne la mise en place d'une évaluation structurelle, qui prendrait la forme d'un contrôle indépendant réalisé tous les cinq ans par des instances universitaires.

Si ces recommandations politiques sont suivies, le système gagnera en robustesse et en transparence, et la sécurité juridique sera garantie dans notre pays.

Conclusions stratégiques finales concernant le système irlandais

M. Van Quickenborne conclut en indiquant que le modèle irlandais prouve que la clé de l'efficacité n'est pas le traitement des données à grande échelle. Ce modèle se fonde sur la confiance, plutôt que de la considérer comme un élément accessoire. Il propose également un bon équilibre entre pouvoir et modération. Les autorités peuvent être financièrement transparentes et efficaces sans compromettre le droit à la vie privée des citoyens.

En outre, le modèle irlandais est tourné vers l'avenir. L'Irlande ne fera que renforcer son statut de référence au niveau européen en matière de transparence financière éthique.

Dit alles gebeurt met een brede maatschappelijke consensus. En dat maatschappelijk draagvlak is er eigenlijk niet voor het wetsontwerp dat ter bespreking voorligt. De minister zal waarschijnlijk stellen dat de partijen van de meerderheid het wetsontwerp steunen. Maar is dat werkelijk zo? De minister moet erkennen dat noch zijn eigen partij, noch de MR werkelijk overtuigd is van het voorgestelde systeem.

Verder stelt de heer Van Quickenborne zich de vraag wat de fracties van Les Engagés en cd&v van dit wetsontwerp vinden. Het lid is teleurgesteld dat de aanwezige leden van die fracties hier niet onmiddellijk een antwoord op geven. Het lid betwijfelt ook of de leden van de overige meerderheidspartijen werkelijk achter dit wetsontwerp staan.

Welnu, het lid stelt die vragen omdat de uitdaging van het CAP niet in de uitbreiding ervan ligt, maar in het behoud van het evenwicht. Voor de leden die twijfelen, biedt het Ierse model een voorbeeld van hoe een moderne rechtsstaat financiële integriteit kan waarborgen zonder de fundamentele rechten te ondermijnen. Zoals in België, bestaat er in andere landen een grote spanning tussen efficiëntie en privacy, maar Ierland heeft die spanning verzoend in het ISBAR-systeem. Dat is geen databank, maar een digitaal anker van de rechtsstaat: een instrument dat aantoont dat de strijd tegen witwassen, corruptie en georganiseerde fraude niet hoeft te botsen met de bescherming van de menselijke waardigheid.

Het lid vangt vervolgens de bespreking aan van het Luxemburgse model, dat eveneens inspiratie kan bieden. Dat geldt des te meer nu de eerste minister pleit voor een nauwere samenwerking op Benelux-niveau. Het lid is overigens van mening dat het Nederlandse en het Luxemburgse model op het vlak van het CAP en *money control* richtinggevend zouden moeten zijn voor België.

Opmerkelijk is dat Luxemburg heel wat Belgische wetgeving quasi kopieert, maar dat dit niet het geval is wat betreft het CAP. Luxemburg is hierbij een andere weg ingeslaan, met een eigen centraal register: registre des comptes de paiements et des comptes bancaires (RCPCB, hierna verkort tot RCP). Het lid schetst nog nader de historische context (de zgn. “couponknippers”) en de wettelijke basis van het register (de wet van 18 december 2015), die voortvloeit uit de omzetting van de vierde anti-witwasrichtlijn (AML4, of Richtlijn (EU) 2015/849).

Het Luxemburgse RCP betreft een volledig digitaal systeem dat dagelijks wordt geüpdatet en dat uitsluitend raadpleegbaar is op aanvraag. Het centraal register wordt

Le système irlandais fait l'objet d'un large consensus social – une adhésion qui manque au projet de loi à l'examen. Le ministre affirmera probablement que les groupes de la majorité soutiennent le projet de loi. Mais est-ce vraiment le cas? Le ministre doit reconnaître que ni son propre groupe, ni le groupe MR ne sont totalement convaincus par le système proposé.

Ensuite, M. Van Quickenborne se demande ce que les groupes Les Engagés et cd&v pensent de ce projet de loi. Il est déçu que les membres présents de ces groupes ne répondent pas immédiatement. Le membre doute également du soutien que les membres des autres partis de la majorité apportent à ce projet de loi.

En réalité, si le membre pose ces questions, c'est parce que le défi que le PCC doit relever ne réside pas dans son expansion, mais bien dans la préservation de l'équilibre. Pour les membres qui auraient des doutes, le modèle irlandais illustre comment un État de droit moderne peut garantir l'intégrité financière sans porter atteinte aux droits fondamentaux. Comme la Belgique, d'autres pays connaissent une forte tension entre efficacité et protection de la vie privée, mais l'Irlande est parvenue à concilier ces deux aspects dans le système ISBAR. Ce n'est pas une banque de données, mais bien un ancrage numérique de l'État de droit: un outil qui montre que la lutte contre le blanchiment, la corruption et la fraude organisée n'est pas nécessairement incompatible avec la protection de la dignité humaine.

Ensuite, le membre initie la discussion sur le modèle luxembourgeois, une autre source d'inspiration potentielle. C'est d'autant plus vrai que le premier ministre plaide pour un renforcement de la collaboration au niveau du Benelux. Le membre est d'ailleurs d'avis que les modèles néerlandais et luxembourgeois devraient servir de référence à la Belgique pour le PCC et le *money control*.

Il est à noter que le Luxembourg copie, pour ainsi dire, une grande partie de la législation belge, mais que ce n'est pas le cas en matière de PCC. Le Luxembourg a choisi une autre voie, celle d'un registre central propre: le registre des comptes de paiements et des comptes bancaires (RCPCB, ci-après abrégé en “RCP”). Le membre revient sur le contexte historique (les “coupeurs de coupons”) et sur la base légale du registre (la loi du 18 décembre 2015), qui découle de la transposition de la quatrième directive antiblanchiment (AML4 ou directive (EU) 2015/849).

Le RCP luxembourgeois est un système entièrement numérique, quotidiennement mis à jour et qui n'est consultable que sur demande. Le registre central est

beheerd door de fiscus, in nauwe samenwerking met de financiële sector en de centrale bank. Datamining, geautomatiseerde profilering en risicoscoring zijn expliciet verboden. Zo combineert het Luxemburgse systeem de volledige traceerbaarheid, met maximale gegevensbescherming. Het is dus een model van transparantie op verzoek.

In Luxemburg stond nochtans traditioneel het bankgeheim centraal. De automatische uitwisseling van bankinformatie werd er geweigerd, aangezien gegevens enkel op verzoek werden verstrekt. Verschillende factoren hebben het land ertoe aangezet dit rigide bankgeheim op te heffen, zoals de oprichting van de Financial Action Task Force (FATF) in 1989 en de financiële crisis van 2008. In dat verband kan ook verwezen worden naar het OESO-project *Base Erosion and Profit Shifting* (BEPS).

Vervolgens aanvaardde Luxemburg in 2014 de *Common Reporting Standard* (CRS), een internationale standaard die de automatische fiscale informatie-uitwisseling regelt tussen de EU- en OESO-landen. Met deze stap engageerde Luxemburg zich om bankgegevens van buitenlandse rekeninghouders systematisch te delen, waardoor het traditionele bankgeheim definitief werd doorbroken en fiscale transparantie aanzienlijk werd versterkt.

Een volgende stap was de vierde anti-witwasrichtlijn (AML4) uit 2015, die lidstaten verplicht om een nationaal rekeningregister op te zetten. Zoals aangehaald, werd die richtlijn nog datzelfde jaar omgezet in de Luxemburgse wetgeving, met inwerkingtreding op 1 januari 2016. Dat contrasteert met de omzettingen in de Belgische wetgeving, die vaak lang op zich laten wachten.

Overigens heeft ook de Europese spaarrichtlijn 2003/48/EG, die in 2005 in werking trad, een belangrijke rol gespeeld, onder meer om een einde te maken aan de zogenaamde couponknippers. Die richtlijn had tot doel belastingontwijking door particulieren tegen te gaan: de lidstaten moesten ofwel kiezen voor gegevensuitwisseling (waarbij landen elkaar op de hoogte brachten van ontvangen interesten door buitenlanders), ofwel voor een bronheffing (waarbij de belasting onmiddellijk aan de bron werd ingehouden).

Zo bedroeg de bronheffing in Luxemburg 35 % sinds 2011. Driekwart van deze heffing ging naar het land van herkomst van de betrokken persoon, terwijl een kwart naar het land ging waar die persoon de interesten had geïnd. Binnen die regeling bleef de buitenlander anoniem voor de fiscus van zijn thuisland.

géré par le fisc, en étroite collaboration avec le secteur financier et la banque centrale. Le *data mining*, le profilage automatisé et l'évaluation des risques des contribuables sont expressément interdits. Le système luxembourgeois combine ainsi une traçabilité complète et une protection maximale des données. C'est donc un modèle de transparence à la demande.

Le secret bancaire était pourtant traditionnellement au cœur du système luxembourgeois. L'échange automatique d'informations bancaires y était refusé, car les données n'étaient fournies que sur demande. Plusieurs événements ont amené le Luxembourg à lever ce secret bancaire rigide, par exemple l'action du Groupe d'action financière (GAFI) en 1989 et la crise financière de 2008. L'intervenant cite également le projet OCDE *Base Erosion and Profit Shifting* (BEPS).

Ensuite, en 2014, le Luxembourg a accepté la norme internationale *Common Reporting Standard* (CRS) régissant l'échange automatique d'informations fiscales entre les pays de l'Union européenne et les pays de l'OCDE. Le Luxembourg s'est ainsi engagé à communiquer systématiquement les données bancaires des titulaires de compte étrangers, rompant ainsi définitivement avec la tradition du secret bancaire et renforçant considérablement la transparence fiscale.

Une étape supplémentaire a été franchie dès l'introduction de la quatrième directive anti-blanchiment (AML4) de 2015, qui impose aux États membres de créer un registre national des comptes. Comme indiqué précédemment, la même année, cette directive fut déjà transposée dans la législation luxembourgeoise, et elle est entrée en vigueur le 1^{er} janvier 2016. L'intervenant souligne le contraste avec les transpositions en droit belge, qui se font souvent attendre un bon moment.

Par ailleurs, la directive européenne sur l'épargne 2003/48/CE, entrée en vigueur en 2005, a également joué un rôle important, notamment en vue de mettre fin au "découpage de coupons". Cette directive visait à lutter contre l'évasion fiscale par les particuliers: les États membres ont dû opter soit pour un échange de données (les pays s'informant mutuellement des intérêts perçus par les étrangers) soit pour un prélèvement à la source (imposition prélevée directement à la source).

Ainsi, le prélèvement à la source atteignait 35 % au Luxembourg depuis 2011. Trois quarts de ce prélèvement allaient au pays d'origine de la personne concernée et un quart au pays où cette personne avait perçu ces intérêts. Dans ce régime, l'étranger restait anonyme pour le fisc de son pays d'origine.

Daarentegen koos de grote meerderheid van de landen vanaf het begin voor gegevensuitwisseling. België sloot zich daarbij aan in 2010, waardoor er uiteindelijk slechts twee Europese landen overbleven met het systeem van bronheffing: Luxemburg en Oostenrijk. Particulieren moesten in dat kader een afweging maken tussen netto meer overhouden of hun anonimiteit behouden. In 2015 koos Luxemburg uiteindelijk voor de gegevensuitwisseling, en later volgde ook Oostenrijk. Om te voorkomen dat men zou uitwijken naar fiscaalvriendelijke paradijzen, werd dit principe bovendien afgedwongen bij tien geassocieerde gebieden buiten de EU, waaronder de Kaaimaneilanden en Zwitserland.

Die gegevensuitwisseling onder de Europese spaarrichtlijn viseert de interesten van spaarboekjes, zichtrekeningen, termijnrekeningen, kasbons en obligaties. Ook producten die onrechtstreeks interestinkomsten genereren, zoals bepaalde beleggingsfondsen, vallen onder dit systeem. Daarbij moeten twee voorwaarden vervuld zijn. Ten eerste moet het gaan om fondsen met een Europees paspoort. Ten tweede moet het fonds minstens een bepaald percentage beleggen in schuldvorderingen (bijvoorbeeld obligaties). Bij een beleggingsfonds waarbij de opbrengsten worden uitgekeerd in dividenden, wordt informatie over de coupon uitgewisseld zodra het fonds minstens 15 % in obligaties belegt. Bij een kapitalisatiefonds (een fonds dat geen dividenden uitkeert), wordt er informatie uitgewisseld wanneer het fonds minstens 25 % in obligaties belegt.

Zo blijven de dividenden en meerwaarden op aandelen voorlopig buiten schot, al wordt daar intussen ook aan gesleuteld. Evenmin wordt informatie uitgewisseld over fondsen met een Europees paspoort die minder dan de vastgelegde percentages in schuldvorderingen beleggen. Bovendien vallen alle fondsen zonder Europees paspoort en gestructureerde producten buiten het toepassingsgebied. Ook verzekeringsproducten zoals tak 21 en tak 23 blijven uitgesloten, al is de kans groot dat dit in de toekomst zal wijzigen. Zo ligt er al sinds 2009 een voorstel van richtlijn op tafel om het toepassingsgebied uit te breiden tot gestructureerde producten en verzekeringsproducten.

Volgens experts had de opheffing van het bankgeheim in Luxemburg nog een ander gevolg. De informatieoverdracht was initieel weliswaar beperkt tot de interestinkomsten, maar de verwachting was dat dit vrij snel zou uitmonden in een volledige gegevensuitwisseling. Intussen is dat ook gebeurd. De vraag rees vervolgens of er nog landen waren waar men naartoe kon uitwijken, gelet op de situatie in Luxemburg. Zwitserland bleek op dat moment nog steeds een mogelijke vluchtroute te zijn. Fiscalisten

À l'inverse, la plupart des pays ont opté, dès le départ, pour l'échange des données. La Belgique l'a fait en 2010, réduisant ainsi finalement à deux le nombre de pays européens à appliquer le système de prélèvement à la source, à savoir le Luxembourg et l'Autriche. Les particuliers ont alors dû choisir entre un revenu net plus élevé ou le maintien de leur anonymat. En 2015, le Luxembourg a finalement opté pour l'échange des données et l'Autriche lui a ensuite emboîté le pas. En outre, afin d'éviter que les contribuables recherchent un refuge dans des paradis fiscaux, ce principe a été imposé à dix territoires associés en dehors de l'Union européenne, par exemple aux Îles Caïmans et à la Suisse.

Cet échange de données visé par la directive européenne sur l'épargne concerne les intérêts issus des livrets d'épargne, des comptes à vue, des comptes à terme, des bons de caisse et des obligations. Les produits qui génèrent des intérêts indirects, tels que certains fonds d'investissement, sont également visés par ce système. Deux conditions doivent être remplies. D'une part, ces fonds doivent disposer d'un passeport européen. D'autre part, un certain pourcentage minimal des fonds doit être investi dans des créances (par exemple dans des obligations). Pour un fonds d'investissement dont les revenus sont distribués sous la forme de dividendes, les informations sur les coupons sont échangées dès qu'au moins 15 % sont investis dans des obligations. Pour les fonds de capitalisation (qui ne distribuent pas de dividendes), les informations sont échangées lorsque le fonds investit au moins 25 % dans des obligations.

Les dividendes et les plus-values sur actions ne sont donc provisoirement pas encore visés, mais un mécanisme visant à les incorporer est en cours de conception. De même, aucune information n'est échangée à propos des fonds disposant d'un passeport européen et investis dans des créances à raison d'un pourcentage inférieur au seuil prévu. En outre, les fonds sans passeport européen et les produits structurés ne sont pas visés. Les produits d'assurance tels que les branches 21 et 23 restent également exclus du champ d'application, même si cela va très certainement changer. En effet, une proposition de directive visant à intégrer les produits structurés et les produits d'assurance est sur la table depuis 2009.

Selon les experts, la suppression du secret bancaire au Luxembourg a eu une autre conséquence. Certes, la communication d'informations se limitait initialement aux revenus perçus sous la forme d'intérêts, mais les observateurs s'attendaient à ce que cela débouche rapidement sur un échange généralisé d'informations. Et c'est ce qui s'est arrivé. La question s'est alors posée de savoir s'il existait encore des pays vers lesquels se tourner, compte tenu de la situation au Luxembourg. À ce

wezen er echter op dat ook daar de mazen van het net zouden worden gedicht. Dat was destijds eveneens de stelling van fiscaal advocaat Typhanie Afschrift.

Tot slot is het ook belangrijk dat bij de Europese spaarrichtlijn het achterpoortje van de schijnvennootschappen werd gesloten. Zo viseerde de uitbreiding van de richtlijn de gegevensuitwisseling van fiscaalvriendelijke tussenstructuren, stichtingen en trusts.

Daarnaast voerden ook de Verenigde Staten de druk op om steeds meer informatie uit te wisselen. Zo kwam er de FATCA-wetgeving (*Foreign Account Tax Compliance Act*), die banken in andere landen verplichtte fiscale gegevens van Amerikaanse belastingplichtigen automatisch door te geven aan de Amerikaanse fiscus. Deze wet inspireerde vijf grote Europese landen om te onderzoeken in hoeverre een Europese variant van FATCA haalbaar was. Dat zou betekenen dat Europeanen ook buiten Europa niet langer konden uitwijken.

Vervolgens komt de heer Van Quickenborne terug tot de Luxemburgse wet van 18 december 2015, die overigens unaniem werd aangenomen. In de toelichting bij die wet werden er drie doelstellingen geformuleerd: (i) de fiscale transparantie, (ii) de witwasbestrijding, en (iii) de bescherming van de persoonlijke levenssfeer. Zo vormt het Luxemburgse RCP een hybride instrument: het garandeert dat Luxemburg voldoet aan Europese normen zonder het fundamentele principe van de bankdiscretie te schenden.

Voorts bepaalt het Luxemburgse wettelijk kader de definities en de modaliteiten die verband houden met het centrale register. Het lid gaat vervolgens dieper in op de driedelige institutionele structuur.

Ten eerste gebeurt het beheer van het centrale register door de Administration des contributions directes (ACD). Dat is een afdeling binnen het Luxemburgse ministerie van Financiën, die zorgt voor de technische en administratieve verwerking. ACD beheert de centrale server, voert kwaliteitscontroles uit op de aangeleverde gegevens, en verwerkt de toegangsaanvragen van bevoegde autoriteiten. ACD beschikt over ongeveer 25 specialisten in IT, compliance en juridische aangelegenheid. Het budget werd vastgelegd op 3,8 miljoen euro in 2025. Het lid wenst dan ook van de minister te vernemen wat het budget is van het Belgische CAP?

moment-là, la Suisse restait une échappatoire possible. Toutefois, les fiscalistes ont souligné que les mailles du filet allaient également y être comblées. C'était notamment la position de l'avocate fiscaliste Typhanie Afschrift.

Enfin, il est également important de souligner que la directive européenne sur l'épargne a mis fin au recours aux sociétés-écrans. Ainsi, l'extension du champ d'application de la directive visait en effet l'échange de données de structures intermédiaires, de fondations et de trusts fiscalement avantageux.

De plus, les États-Unis ont également intensifié la pression en vue d'obtenir l'échange de plus en plus d'informations. Par exemple, la législation FATCA (*Foreign Account Tax Compliance Act*) a été adoptée, laquelle impose aux banques installées à l'étranger de communiquer automatiquement les données fiscales des contribuables américains au fisc américain. Cette loi a incité cinq grands pays européens à examiner dans quelle mesure une variante européenne de la FATCA était réalisable. Cela signifierait que les Européens ne pourraient plus trouver de refuge fiscal en dehors de l'Europe non plus.

M. Van Quickenborne revient ensuite sur la loi luxembourgeoise du 18 décembre 2015, qui a d'ailleurs été adoptée à l'unanimité. Dans l'exposé des motifs de cette loi, trois objectifs ont été formulés: (i) la transparence fiscale, (ii) la lutte contre le blanchiment d'argent et (iii) la protection de la vie privée. Le RCP luxembourgeois constitue ainsi un instrument hybride: il veille à ce que le Luxembourg satisfasse aux normes européennes sans pour autant transgresser le principe fondamental de la discrétion bancaire.

Par ailleurs, le cadre légal luxembourgeois reprend les définitions et les modalités liées au registre central. Le membre s'attarde ensuite sur la structure institutionnelle tridimensionnelle.

Premièrement, la gestion du registre central est assurée par l'Administration des contributions directes (ACD). Il s'agit d'une division du ministère des Finances luxembourgeois qui est chargée du traitement technique et administratif. L'ACD assure la gestion du serveur central, effectue des contrôles de qualité sur les données fournies et traite les demandes d'accès introduites par les autorités compétentes. L'ACD dispose d'environ 25 spécialistes dans les domaines de l'informatique, de la conformité (*compliance*) et des affaires juridiques. Son budget a été fixé à 3,8 millions d'euros en 2025. Le membre souhaite dès lors savoir quel est le budget prévu pour le PCC belge.

Ten tweede wordt het toezicht uitgeoefend door de Commission nationale pour la protection des données (CNPD). Deze instantie vervult drie rollen: (i) de vergunningsverlening (de goedkeuring van de gegevensverwerking door het ACD), (ii) het ex post toezicht (de jaarlijkse controle op proportionaliteit en veiligheid), en (iii) de klachtenbehandeling (de inzage- of correctieverzoeken). Uit een recent verslag van de CNPD blijkt dat het Luxemburgse centraal register een evenwicht inhoudt tussen effectiviteit en gegevensbescherming.

Een derde actor is de *Cellule de renseignement financier* (CRF), die ondergebracht is bij het Luxemburgse parket. Deze institutionele inbedding kan ook als voorbeeld dienen voor de Belgische CFI, die voorlopig nog is ingebed in de FOD Financiën. De CRF heeft toegang tot het register voor onderzoeken naar witwaspraktijken en terrorismefinanciering. Zij beschikt niet over een rechtstreeks recht op data-export, maar kan via protocollen informatie uitwisselen met buitenlandse tegenhangers binnen de Egmont-groep.

Verder bespreekt het lid de toegangs- en raadplegingsprocedure van het Luxemburgse register.

Zo zijn er maar drie instanties die het Luxemburgse register kunnen consulteren, vergeleken met tien in België en vijf in Ierland. Het betreft de ACD (voor belastingsonderzoeken en internationale verzoeken), de CRF (voor de voormelde onderzoeken) en de gerechtelijke autoriteiten (op basis van een rechterlijk bevel). De Luxemburgse wetgever heeft de toegang dus in die mate beperkt dat andere instanties hiertoe onbevoegd zijn (zoals politie- en sociale diensten, alsook gemeenten).

Bij de raadplegingsprocedure zijn vijf stappen te onderscheiden: (i) de aanvraag via het beveiligde portaal, (ii) de controle door het ACD, (iii) de beperkte zoekopdracht ter identificatie van de persoon of onderneming, (iv) de lijst van rekeningen met vermelding van de bank en de datum van opening en sluiting van de rekening, en (v) de logging en archivering gedurende maximaal tien jaar. Hierbij is er een gelijkenis tussen het Belgische en Luxemburgse systeem. Tot slot bedraagt de doorlooptijd voor een standaardaanvraag gemiddeld minder dan een uur.

De heer Van Quickenborne somt vervolgens de gegevens op die financiële instellingen dienen te verstrekken aan het RCP, de Luxemburgse tegenhanger van het CAP. De verplichte gegevensvelden zijn:

— de identificatie van de rekeninghouder;

Deuxièmement, la surveillance est exercée par la Commission nationale pour la protection des données (CNPD). Cette instance remplit trois rôles: (i) l'octroi d'autorisations (approbation du traitement des données par l'ACD), (ii) le contrôle ex post (contrôle annuel de la proportionnalité et de la sécurité) et (iii) le traitement des plaintes (demandes de consultation ou de correction). En outre, un rapport récent de la CNPD révèle que le registre central luxembourgeois parvient à maintenir un équilibre entre, d'une part, l'efficacité et, d'autre part, la protection des données.

Un troisième acteur est la Cellule de renseignement financier (CRF), rattachée au parquet luxembourgeois. Ce cadre institutionnel pourrait également servir d'exemple pour la CTIF belge, qui reste pour l'instant intégrée au SPF Finances. La CRF a accès au registre pour ses enquêtes sur les pratiques de blanchiment et sur le financement du terrorisme. Elle ne dispose pas d'un droit direct d'exportation des données, mais peut, via des protocoles, échanger des informations avec des homologues étrangers au sein du groupe Egmont.

Le membre aborde ensuite la procédure d'accès et de consultation du registre luxembourgeois.

Seules trois instances sont habilitées à consulter ce registre, contre dix en Belgique et cinq en Irlande. Il s'agit de la CGPD (pour les enquêtes fiscales ainsi que les demandes internationales), de la CRF (pour les enquêtes susmentionnées) et des autorités judiciaires (sur la base d'une ordonnance du juge). Le législateur luxembourgeois a ainsi limité l'accès de telle sorte que d'autres instances (comme la police, les services sociaux et les communes) en sont exclues.

La procédure de consultation se déroule en cinq étapes distinctes: (i) la demande via le portail sécurisé, (ii) le contrôle par la CGPD, (iii) la recherche limitée visant à identifier la personne ou l'entreprise, (iv) la liste des comptes, mentionnant la banque et les dates d'ouverture et de fermeture du compte, (v) la journalisation et l'archivage pendant une durée maximale de dix ans. Il existe en l'occurrence une similitude entre les systèmes belge et luxembourgeois. Enfin, le délai de traitement d'une demande standard est en moyenne inférieur à une heure.

M. Van Quickenborne énumère ensuite les données que les établissements financiers doivent transmettre au RCP, qui est l'équivalent luxembourgeois du PCC. Les champs obligatoires contiennent des données concernant:

— l'identification du titulaire du compte;

- het nationaal identificatienummer;
- het IBAN-nummer;
- de betrokken instelling;
- de openings- en sluitingsdata;
- de lijst van de volmachthouders; en
- het type van de rekening.

Wat de technische infrastructuur betreft, meldt het lid dat de data worden gehost in de overheidscloud van het *Centre de Technologie de l'Information de l'État* (CTIE). Back-ups worden bewaard in twee verschillende datacenters. Encryptie gebeurt via het systeem *LuxTrust*. De verbindingen tussen banken en de ACD gebruiken een beveiligd kanaal, genaamd *Luxfile*, mét digitale handtekening.

Inzake datakwaliteit en validatie, legt het lid uit dat de ACD elke upload controleert op formaat- en consistentiefouten. Het aantal rekeningrecords in Luxemburg bedraagt 11 miljoen, verspreid over ca. 85 instellingen. Daarin zitten niet de saldi en mogelijk ook niet de financiële contracten.

De bewaartermijn bedraagt vijf jaar. Daarna worden de gegevens automatisch verwijderd of geanonimiseerd voor statistische doeleinden.

Bij wijze van tussentijdse conclusie stelt de heer Van Quickenborne dat het RCP een efficiënt en veilig aanspreekpunt is, dat beschikt over een robuuste juridische basis en waarbij de balans tussen toegankelijkheid en privacy zorgvuldig wordt bewaakt. Alleen bevoegde instanties hebben toegang.

De heer Van Quickenborne roept de vice-eersteminister op om dit dossier te bespreken met zijn Luxemburgse ambtsgenoot, de heer Gilles Roth. In Luxemburg bestaat die datamining niet. In ons land is het coalitiepartner Vooruit die aanstuurt op het organiseren van zulke massale surveillance. Daartegen verzet Open Vld zich principieel en ten stelligste.

Luxemburg heeft de goede aspecten van het Belgisch model overgenomen, en de slechte – het systeem van *money control* – achterwege gelaten.

De heer Wim Van der Donckt (N-VA) werpt op dat Luxemburg in 2020 een wet heeft aangenomen waarin datamining, weliswaar onder strikte voorwaarden, wel

- le numéro d'identification national;
- le numéro IBAN;
- l'établissement concerné;
- les dates d'ouverture et de clôture;
- la liste des mandataires; et
- le type de compte.

En ce qui concerne l'infrastructure technique, le membre indique que les données sont hébergées dans le *cloud* administré par le Centre de Technologie de l'Information de l'État (CTIE). Des sauvegardes sont conservées dans deux centres de données distincts. Le chiffrement est assuré par le système *LuxTrust*. Les connexions entre les banques et l'ACD passent par un canal sécurisé, appelé *Luxfile*, qui requiert une signature numérique.

En ce qui concerne la qualité et la validation des données, le membre explique que l'ACD contrôle chaque *upload* afin de détecter toute erreur de format et de cohérence. Au Luxembourg, le nombre d'enregistrements de comptes s'élève à 11 millions, répartis sur environ 85 établissements. Les soldes n'y figurent pas, et peut-être pas non plus les contrats financiers.

La durée de conservation est de cinq ans. Au-delà de ce délai, les données sont automatiquement effacées ou anonymisées à des fins statistiques.

En guise de conclusion intermédiaire, M. Van Quickenborne indique que le RCP est un point de contact efficace, sécurisé, fondé sur une base juridique solide et qui permet d'assurer soigneusement un équilibre entre l'accessibilité et la protection de la vie privée. Seules les autorités compétentes y ont accès.

M. Van Quickenborne invite le vice-premier ministre à en débattre avec son homologue luxembourgeois, M. Gilles Roth. Au Luxembourg, il n'existe pas d'exploration de données. Dans notre pays, c'est le partenaire de coalition Vooruit qui souhaite la mise en place d'une surveillance de masse de ce type. L'Open Vld s'y oppose, par principe et avec la plus grande fermeté.

Le Luxembourg a repris les points positifs du modèle belge et il a laissé ses points négatifs de côté, à savoir le système de *money control*.

M. Wim Van der Donckt (N-VA) fait observer qu'en 2020, le Luxembourg a adopté une loi autorisant l'exploration de données, mais à des conditions strictes. En

toegelaten is. In 2023 werd die wetgeving uitgebreid, waardoor het gebruik van AI-toepassingen en algoritmes wordt toegelaten. Wat de heer Van Quickenborne vertelt, klopt dus niet.

De heer Vincent Van Quickenborne (Open Vld) werpt tegen dat datamining in Luxemburg – en ook bij ons is dat trouwens reeds het geval – wordt losgelaten op gegevens die belastingplichtigen spontaan delen met de fiscus, wel wetende dat die gegevens kunnen worden uitgevlooid. Hier gaat het echter over gegevens die niet worden gedeeld met de fiscus en die worden bekendgemaakt in het CAP met de enkele bedoeling om het banktoezicht te faciliteren.

De heer Wim Van der Donckt (N-VA) wijst op het gevaar van “hallucinaties” dat ingebakken zit in AI-toepassingen. AI-oplossingen kunnen resultaten afleveren die overtuigend lijken, maar halve waarheden en zelfs leugens bevatten. Ook het discours van de heer Van Quickenborne is doorspekt met halve waarheden. Hij vertelt niet het hele verhaal.

De heer Vincent Van Quickenborne (Open Vld) nodigt de heer Van der Donckt uit om een concreet voorbeeld te geven van een halve waarheid die hij in de loop van zijn uitgebreid betoog betreffende de voorliggende tekst verkondigd zou hebben.

Wat AI betreft, is de hamvraag de volgende: gebruikt de fiscus vandaag AI? De vice-eersteminister heeft die vraag tijdens de bespreking tot tweemaal toe ontkennend beantwoord. Dat strookt evenwel niet met het antwoord van de vice-eersteminister op de schriftelijke vraag nr. 132 inzake “Transparantie over het gebruik van datamining door de FOD Financiën” die het lid indiende 24 maart 2025. In zijn antwoord van 28 april 2025 verklaarde de minister onder meer het volgende: “De FOD Financiën gebruikt momenteel de programma’s VDMML en e-Miner van SAS” (QRVA 56.012, p. 323). Die programma’s berusten wel degelijk op AI.

De heer Wim Van der Donckt (N-VA) voert aan dat de heer Van Quickenborne ten onrechte beweerde dat datamining in Luxemburg niet werd toegepast.

De heer Vincent Van Quickenborne (Open Vld) geeft aan dat hij zijn redenering omtrent het Luxemburgse model nog aan het ontwikkelen is. Men mag geen appels met peren vergelijken. Uiteraard bestaat datamining ook in Luxemburg. Maar de hamvraag is: wordt het toegepast op vrijwillig bezorgde gegevens, zoals ginds en ook hier reeds het geval is, of op onvrijwillige data, zoals men hier wil invoeren? *Datamining* wordt in België al sinds 2012 toegepast. Wat hier ter discussie voorligt, is het

2023, l’application de cette législation a été étendue et, depuis lors, l’utilisation d’applications IA et d’algorithmes est autorisée. Les propos de M. Van Quickenborne ne sont donc pas exacts.

M. Vincent Van Quickenborne (Open Vld) répond qu’au Luxembourg, l’exploration de données est appliquée aux données que les contribuables partagent spontanément avec le fisc – comme en Belgique aujourd’hui, d’ailleurs – tout en sachant que ces données pourront être épluchées. Le texte à l’examen porte quant à lui sur des données qui n’auront pas été communiquées au fisc et qui seront publiées dans le PCC dans le seul but de faciliter la surveillance bancaire.

M. Wim Van der Donckt (N-VA) souligne le risque d’“hallucination” inhérent aux applications IA. Les solutions IA peuvent en effet donner des résultats qui paraissent convaincants, mais qui contiennent des demi-vérités, voire des mensonges, tout comme le discours de M. Van Quickenborne, qui est également truffé de demi-vérités et qui passe certains points sous silence.

M. Vincent Van Quickenborne (Open Vld) demande à M. Van der Donckt de donner un exemple concret de demi-vérité qu’il aurait dite au cours de son long exposé.

S’agissant de l’IA, la question essentielle est la suivante: le fisc recourt-il actuellement à l’IA? Le vice-premier ministre y a répondu par la négative, à deux reprises, au cours de la discussion. Cela ne concorde toutefois pas avec la réponse du vice-premier ministre à la question écrite n° 132 relative à la “Transparence sur l’utilisation du *data mining* par le SPF Finances” que le membre a déposée le 24 mars 2025. Dans sa réponse du 28 avril 2025, le ministre a notamment déclaré: “Le SPF Finances utilise actuellement les programmes VDMML et e-Miner de l’entreprise SAS.” (QRVA 56.012, p. 323). Ces programmes font en effet bien appel à l’IA.

M. Wim Van der Donckt (N-VA) soutient que M. Van Quickenborne s’est trompé lorsqu’il a affirmé qu’il n’est pas fait usage de l’exploration de données au Luxembourg.

M. Vincent Van Quickenborne (Open Vld) indique qu’il est encore en train d’exposer son raisonnement concernant le modèle luxembourgeois. Il ne faut pas comparer des pommes et des poires. Il va de soi que l’exploration de données existe aussi au Grand-Duché de Luxembourg, mais la question essentielle est la suivante: Est-elle appliquée à des données transmises volontairement, comme au Luxembourg et en Belgique, ou involontairement, comme le souhaite le texte à

toepassen van datamining op bankgegevens die de banken bezorgd hebben aan het CAP.

Het lid zet zijn uiteenzetting van het Luxemburgse model verder met het luik toezicht, controle en verantwoording. De ACD valt onder het ministerie van Financiën. De wet van 2015 verplicht de minister jaarlijks een verslag voor te leggen aan het Parlement. Overigens zit die verplichting ook vervat in onze wet van 2011, maar wordt hieraan geen gevolg gegeven.

Overeenkomstig de Luxemburgse wet dient het verslag de volgende informatie te bevatten:

- het aantal raadplegingen;
- de instellingen die gegevens hebben aangeleverd;
- de technische storingen;
- de auditbevindingen.

Het Luxemburgse Rekenhof kan op verzoek van de commissie voor Financiën een financiële en operationele audit uitvoeren. Tot op heden is het register elk jaar als conform en efficiënt beoordeeld.

De rol van de *Commission Nationale pour la Protection des Données* (CNPD) is volledig onafhankelijk. Zij houdt toezicht op de naleving van de AVG en op de Luxemburgse wet van 1 augustus 2018 betreffende de bescherming van de persoonsgegevens. Anders dan de GBA bij ons, heeft de CNPD volledige toegang tot de logbestanden van het RCP en kan ze steekproefsgewijs nagaan of raadplegingen gerechtvaardigd waren. De CNPD kan als autoriteit ook bindende instructies geven aan de ACD of aan de CRF, en zij heeft ook de macht om boetes op te leggen. In haar verslag van 2024 onderstreepte de CNPD dat het register niet mag evolueren van een identificatie- naar een analyse-instrument.

Met betrekking tot parlementaire controle licht de heer Van Quickenborne toe dat de Luxemburgse commissie voor Financiën jaarlijks een hoorzitting houdt met de minister van Financiën en met de directeur van de ACD, gewijd aan het RCP. Dat staat in schril contrast met de situatie bij ons, waar de verantwoordelijken van het CAP begin 2026 voor de eerste keer door het Parlement zullen worden gehoord. In de commissie van Justitie van Luxemburg wordt de procuratiehouder van de CRF gehoord wanneer het gebruik van het register bij strafonderzoeken ter sprake komt. Het RCP geniet brede parlementaire steun als noodzakelijk instrument

l'examen? L'exploration de données est appliquée en Belgique depuis 2012, mais la discussion actuelle porte sur l'exploration des données bancaires transmises au PCC par les banques.

Le membre poursuit son exposé sur le modèle luxembourgeois en évoquant le volet relatif à la surveillance, au contrôle et à la justification. L'ACD relève du ministère des Finances et la loi de 2015 oblige le ministre à soumettre chaque année un rapport au Parlement. Notre loi de 2011 prévoit d'ailleurs également cette obligation, mais elle n'est pas respectée.

La loi luxembourgeoise prévoit que ce rapport doit contenir des informations sur:

- le nombre de consultations;
- les établissements qui ont fourni des données;
- les dysfonctionnements techniques;
- les constatations d'audit.

À la demande de la commission des Finances, la Cour des comptes luxembourgeoise peut réaliser un audit financier et opérationnel. Jusqu'à présent, le registre a chaque année été jugé conforme et efficace.

La *Commission nationale pour la protection des données* (CNPD) est tout à fait autonome. Elle veille au respect du RGPD et de la loi luxembourgeoise du 1^{er} août 2018 relative à la protection des données à caractère personnel. Contrairement à notre Autorité de protection des données, la CNPD a pleinement accès aux fichiers de journalisation du RCP et peut procéder à des coups de sonde pour vérifier si les consultations étaient justifiées. La CNPD peut également, en tant qu'autorité compétente, donner des instructions contraignantes à l'ACD ou à la CRF, et elle dispose du pouvoir d'infliger des amendes. Dans son rapport de 2024, la CNPD a souligné que le registre, qui est un instrument d'identification, ne devait pas devenir un instrument d'analyse.

En ce qui concerne le contrôle parlementaire, M. Van Quickenborne explique que la commission des Finances luxembourgeoise invite chaque année le ministre des Finances et le directeur de l'ACD à une audition consacrée au RCP. Cela contraste fortement avec notre situation. En effet, en Belgique, les responsables du PCC ne seront entendus au Parlement, pour la première fois, qu'au début de l'année 2026. Au Grand-Duché de Luxembourg, le mandataire de la CRF est entendu en commission de la Justice lorsque l'utilisation du registre dans le cadre d'enquêtes pénales est abordée. Le RCP y bénéficie d'un large soutien

in de strijd tegen het witwassen van geld, maar tegelijk hoeft men zich ervoor het RCP te laten uitgroeien tot een surveillancetool.

De Luxemburgse Grondwet beschermt, zoals de Belgische, de privacy. Het Grondwettelijk Hof van Luxemburg verklaarde dat elke geautomatiseerde behandeling van gegevens een uitdrukkelijke wettelijke grondslag vereist en moet onderworpen worden aan een proportionaliteitstoetsing. De wet van 2015 voldoet aan die vereiste, omdat ze het doel van het RCP nauwkeurig bepaalt en elk ander gebruik uitsluit. Het groothertogelijk besluit van 2016 is duidelijk: de data kunnen alleen worden verwerkt met het oog op de identificatie van een bepaalde bankrekening of betaling. Hieruit volgt dat het register niet mag worden gekoppeld aan andere databanken en dat er geen statistische analyse of profilering mag worden op uitgevoerd.

In Luxemburg kan elke burger via het portaal myguichet.lu nagaan of hij voorkomt in het RCP. In België kan dat enkel via de website van het CAP. Het recht op inzage wordt in Luxemburg uitgeoefend via de ACD, die binnen één maand moet antwoorden. Het recht op rectificatie geldt voor onjuistheden in identificatiegegevens. De ACD past veiligheidsnormen toe van verschillende instanties. Het rapport van de CNPD bevestigde dat het register een zeer hoog niveau van technische en organisatorische beveiliging biedt.

De institutionele samenwerking in Luxemburg is groot. Het land telt maar liefst 120 banken en 75 betaaldienstverleners. Elke instelling is verplicht om elke rekeningopening of -sluiting binnen 24 uur te melden. De rapportering gebeurt via het *Luxfile*-portaal dat technisch wordt ondersteund door de Luxemburgse Centrale Bank. Banken zijn aansprakelijk voor onjuiste of laattijdige rapportering en kunnen door de ACD een administratieve boete opgelegd krijgen die kan oplopen tot 125.000 euro. De CRF heeft beperkte toegang tot het register via een beveiligd portaal. Zij mag enkel opzoeken of een persoon een rekening heeft en bij welke instelling. Transactiedetails blijven geheim totdat een rechterlijk bevel is uitgevaardigd. De CRF werkt nauw samen met de ACD en de CNPD.

Luxemburg maakt deel uit van de *Common Reporting Standard*, de CRS, en ook van het Europese *Bank Account Registers Interconnection System* (BARIS). De RCP stuurt niet alleen informatie naar Luxemburgse autoriteiten, maar ook naar buitenlandse partneradministraties via beveiligde kanalen en onder strikte voorwaarden. De gegevens die via BARIS worden gedeeld zijn

parlementaire en tant qu'instrument nécessaire dans la lutte contre le blanchiment d'argent, mais les autorités veillent simultanément à ce qu'il ne devienne pas un outil de surveillance.

À l'instar de la Constitution belge, la Constitution luxembourgeoise protège la vie privée. La Cour constitutionnelle luxembourgeoise a déclaré que tout traitement automatisé de données requiert un fondement légal explicite et doit être soumis à un contrôle de proportionnalité. La loi de 2015 répond à cette exigence, en ce qu'elle définit précisément la finalité du RCP et exclut toute autre utilisation. L'arrêté grand-ducal de 2016 est clair: les données ne peuvent être traitées qu'en vue de l'identification d'un compte bancaire déterminé ou d'un paiement déterminé. Il en découle que le registre ne peut pas être couplé à d'autres bases de données et ne peut servir de base à aucune analyse statistique ni à aucun profilage.

Au Luxembourg, chaque citoyen peut vérifier, via le portail myguichet.lu, s'il apparaît dans le RCP. En Belgique, une telle vérification n'est possible que via le site web du PCC. Au Luxembourg, le droit de consultation est exercé par l'intermédiaire de l'ACD, qui doit répondre dans le mois. Le droit de rectification concerne les erreurs affectant les données d'identification. L'ACD applique les normes de sécurité de différentes instances. Dans son rapport, la CNPD a confirmé que le registre offrait un niveau très élevé de protection technique et organisationnelle.

La coopération institutionnelle est très développée au Luxembourg. Le pays compte pas moins de 120 banques et 75 services de paiement. Chaque institution est obligée de signaler toute ouverture ou fermeture de compte dans les 24 heures. Le signalement est effectué via le portail *Luxfile*, qui est soutenu sur le plan technique par la Banque centrale du Luxembourg. Les banques sont tenues responsables des signalements erronés ou tardifs et peuvent se voir infliger par l'ACD une amende administrative s'élevant jusqu'à 125.000 euros. La CRF a un accès limité au registre via un portail sécurisé. Elle peut uniquement rechercher si une personne dispose d'un compte et auprès de quelle institution. Les détails des transactions restent secrets jusqu'à l'émission d'une injonction judiciaire. La CRF collabore étroitement avec l'ACD et la CNPD.

Le Luxembourg a adhéré à la norme commune de déclaration (NCD) et au système européen d'interconnexion des registres des comptes bancaires (BARIS). Le RCP transmet des informations non seulement aux autorités luxembourgeoises, mais aussi aux administrations partenaires à l'étranger via des canaux sécurisés et dans des conditions strictes. Les données partagées

beperkt tot identificatie. Er vindt geen centrale Europese datamining plaats.

De heer Van Quickenborne belicht vervolgens de operationele resultaten van het Luxemburgse systeem. Volgens het jongste jaarverslag van de ACD waren er in 2024 1,3 miljoen actieve rekeningen in het register. Het register werd 15.000 maal geraadpleegd door bevoegde autoriteiten. Men telde 85 instellingen die dagelijks gegevens aanleveren. De responstijd per query bedraagt gemiddeld twee minuten. Het register werd in meer dan 900 witwas- en belastingonderzoeken gebruikt. Het CRF rapporteerde dat de identificatie van rekeninghouders nu vijf keer sneller gaat dan voor 2016. Het register vervangt dus een tijdrovend proces van manuele bankbevragingen.

In het jaarverslag worden een drietal problemen uitgelicht. Een eerste is het feit dat het register, in tegenstelling tot dat in ons land, geen saldi bevat. Ten tweede zijn er alleen *case-by-case* raadplegingen mogelijk, geen bulkzoekopdrachten. En ten slotte vertraagt het CNPD-toezicht soms een snelle gegevensuitwisseling in urgente zaken. Desondanks oordeelde de Europese Commissie dat het Luxemburgse systeem volledig in overeenstemming is met de Europese AML-richtlijnen.

Sinds de oprichting in 2016 is er een stabiel politiek consensusmodel in Luxemburg uitgebouwd. Het Groothertogdom wil transparant zijn, zonder een controlestaat te worden. Luxemburg werd in 2022 door de *Financial Action Task Force* (FATF) bestempeld als *largely compliant*, met een aanbeveling wat de centrale toegang tot rekeninginformatie betreft. Het model van Luxemburg geldt internationaal als voorbeeld voor landen die de balans zoeken tussen compliance en privacy. Ook de publieke perceptie van het systeem is positief.

In een toekomstig perspectief moet het systeem een hogere capaciteit krijgen en ook snellere API-connecties. Luxemburg onderhandelt voorts met de Europese Commissie over de volledige interconnectie met BARIS voor 2027. Er is verder een versterking gepland van het privacytoezicht. Zo zal er worden ingezet op automatische meldingen bij ongebruikelijke querypatronen, waardoor wordt voorkomen dat bevoegde instanties het register misbruiken voor massaal screenen.

Bij wijze van tweede tussentijdse conclusie stelt de heer Van Quickenborne dat het RCP een efficiënt, stabiel en veilig aanspreekpunt is, dat beschikt over een robuuste juridische basis en waarbij de balans tussen toegankelijkheid en privacy zorgvuldig wordt bewaakt.

via le système BARIS sont limitées à l'identification. Il n'y a pas de *data mining* central au niveau européen.

M. Van Quickenborne présente ensuite les résultats opérationnels du système luxembourgeois. Selon le dernier rapport annuel de l'ACD, en 2024, il y avait 1,3 million de comptes actifs dans le registre, le registre a été consulté 15.000 fois par les autorités compétentes, 85 institutions ont transmis des données quotidiennement et le temps de réponse par requête était de deux minutes en moyenne. Le registre a été utilisé dans plus de 900 enquêtes fiscales et dossiers de blanchiment. Le CRF a révélé que l'identification des titulaires de comptes était aujourd'hui cinq fois plus rapide qu'avant 2016. Le registre remplace donc un processus chronophage de demandes adressées manuellement aux banques.

Le rapport annuel relève trois problèmes. Premièrement, contrairement au système en vigueur dans notre pays, le registre ne reprend pas les soldes. Deuxièmement, il est uniquement possible de consulter des dossiers au cas par cas et non d'effectuer des recherches groupées. Troisièmement, le contrôle de la CNPD empêche parfois un échange de données rapide en cas d'urgence. La Commission européenne a néanmoins jugé que le système luxembourgeois était totalement conforme aux directives anti-blanchiment.

Depuis sa création en 2016, un consensus politique stable s'est établi autour du registre au Luxembourg. Le Grand-Duché veut être transparent sans devenir un État contrôleur. En 2022, le Groupe d'action financière (GAFI) a jugé le modèle luxembourgeois largement conforme, tout en formulant une recommandation sur l'accès centralisé aux informations des comptes. Le modèle luxembourgeois sert d'exemple au niveau international pour les pays qui recherchent l'équilibre entre la conformité et la vie privée. Il jouit également d'une perception publique positive.

Pour l'avenir, le système devra avoir une capacité plus élevée, ainsi que des connexions API plus rapides. Par ailleurs, le Luxembourg négocie avec la Commission européenne en vue d'une interconnexion complète avec le système BARIS pour 2027. Un renforcement du contrôle en matière de vie privée est également prévu. Des messages automatiques seront ainsi envoyés en cas de schémas de requêtes inhabituels de façon à empêcher les instances compétentes de détourner le registre de son utilisation à des fins de screening massif.

En guise de deuxième conclusion intermédiaire, M. Van Quickenborne indique que le RCP constitue un point de contact efficace, stable et sûr, qui s'appuie sur une base juridique robuste veillant à assurer l'équilibre entre l'accessibilité et le respect de la vie privée. Seules

Alleen bevoegde instanties hebben toegang. Er wordt een strikte scheiding tussen identificatie en analyse gehanteerd. Het systeem combineert moderne technologie met constitutionele waarborgen en is in staat zich aan te passen aan de Europese geharmoniseerde AML-omgeving, zonder zijn no-datamining-principe op te geven.

Het lid gaat nader in op de technische werking en de operationele structuur van het systeem. Het Luxemburgse systeem onderscheidt zich van de meeste Europese registers door zijn hoogtechnologische eenvoud. Het verzamelt enkel identificatiegegevens, maar doet dit met maximale nauwkeurigheid en veiligheid. In tegenstelling tot landen die een *big data*-model hanteren, werkt Luxemburg volgens een dataminimalisme-principe: zo weinig mogelijk gegevens, zo snel mogelijk beschikbaar voor wie er wettelijk recht op heeft.

Architectuurgewijs bestaat het RCP uit drie hoofdelementen: de *data collection hub* (het platform waar financiële instellingen hun dagelijkse updates indienen), de *core database* (het centrale opslagpunt beheerd door de bevoegde administratie) en het consultatieportaal waar zich de interface bevindt voor de bevoegde autoriteiten. De drie modules zijn logisch gescheiden, maar fysiek verbonden binnen de beveiligde infrastructuur van het CTIE. De infrastructuur is dubbel uitgevoerd in twee datacenters met een continue synchronisatie. De technologische basis is softwarearchitectuur opgebouwd uit sourcecomponenten met beveiligde middleware.

Wat de datastromen betreft is het zo dat elke financiële instelling dagelijks een xml-bestand verstuurt volgens een bepaalde standaard. De velden zijn strikt gedefinieerd. Ze bevatten geen financiële waarden. De ACD valideert de gegevens via automatische schemacontrole; fouten worden gemeld via het feedbackportaal. Het validatie- en laadproces verloopt in vier fasen: *ingestion*, *validation*, *transformation* en *commit*.

Het consultatieportaal is toegankelijk voor drie categorieën gebruikers: de onderzoekers van de ACD; magistraten en gerechtelijke ambtenaren; en de analisten van de CRF. Gebruikers loggen in met tweefactorauthenticatie. Na succesvolle verificatie kan men een zoekopdracht doen op naam, op identificatienummer of op onderneming. De zoekresultaten tonen de betrokken bankinstelling, het rekeningnummer, de datum van opening en sluiting en, in voorkomend geval, de gevolmachtigde(n). Er worden transacties noch saldi weergegeven. Elke zoekopdracht wordt vooraf gevalideerd

les instances compétentes y ont accès. Une séparation stricte est opérée entre l'identification et l'analyse. Le système combine une technologie moderne avec des garanties constitutionnelles, et il est en mesure de s'adapter à l'environnement européen harmonisé de lutte contre le blanchiment, sans abandonner son refus de principe du *data mining*.

Le membre se penche ensuite sur le fonctionnement technique et la structure opérationnelle du système. Le système luxembourgeois se distingue de la plupart des registres européens par sa simplicité, qui repose sur une technologie de pointe. Il se contente de rassembler des données d'identification, mais il le fait en garantissant une précision et une sécurité maximales. Contrairement aux pays qui adoptent un modèle basé sur des mégadonnées, le Luxembourg applique un principe minimaliste en termes de données: un minimum de données, disponibles le plus rapidement possible pour les instances qui sont autorisées par la loi à les consulter.

Sur le plan architectural, le RCP se compose de trois éléments principaux: le *data collection hub* (la plateforme sur laquelle les institutions financières introduisent leurs mises à jour quotidiennes), la *core database* (le lieu de stockage central géré par l'administration compétente) et le portail de consultation qui contient l'interface pour les autorités compétentes. Ces trois modules sont séparés sur le plan logique, mais reliés physiquement au sein de l'infrastructure sécurisée du CTIE. L'infrastructure a été dédoublée dans deux centres de données synchronisés en continu. La base technologique repose sur une architecture logicielle constituée de composants *source* associés à un intergiciel sécurisé.

En ce qui concerne les flux de données, chaque institution financière envoie chaque jour un fichier xml standardisé. Les champs de ce fichier sont prédéfinis et ne contiennent pas de valeurs financières. L'ACD valide les données à l'aide d'un schéma de contrôle automatique, et les erreurs sont signalées via un portail de *feedback*. Le processus de validation et de chargement se déroule en quatre phases: *ingestion*, *validation*, *transformation* et *commit*.

Le portail de consultation est ouvert à trois catégories d'utilisateurs: les enquêteurs de l'ACD, les magistrats et les fonctionnaires judiciaires, ainsi que les analystes du CRF. Les utilisateurs se connectent à l'aide d'une authentification à deux facteurs. Dès que la connexion est établie, ils peuvent effectuer une recherche par nom, par numéro d'identification ou par entreprise. Les résultats de chaque recherche mentionnent l'établissement bancaire visé, le numéro de compte, la date d'ouverture et de clôture et, le cas échéant, le mandataire ou les mandataires. Les transactions et les soldes ne sont pas

door een automatische rechtencontrole. Het systeem toetst of de gebruiker een actief dossiernummer heeft in het gerechtelijk of fiscaal systeem. Elke (succesvolle of mislukte) query wordt gelogd met diverse gegevens. Die logs worden gedurende een lange termijn (langer dan zes maanden) bewaard. Van de 15.000 raadplegingen die in 2024 werden geregistreerd, was 60 % afkomstig van de fiscus, 25 % van de CRF en 15 % van gerechtelijke instanties.

Het RCP beschikt over meerdere beveiligingslagen. Er is sprake van netwerkbeveiliging, authenticatie, encryptie en *audit trail*. Sleutelbeheer gebeurt door de Luxemburgse Centrale Bank. De ACD beschikt enkel over tijdelijke sleutels voor sessie-encryptie. Dit model voorkomt dat één enkele instantie volledige toegang heeft tot alle data. Het systeem is voorts gebaseerd op *privacy-by-design*-principes. Concrete toepassingen daarvan zijn de minimale datavelden, de automatische verwijdering van inactieve records, de pseudonimisering van logbestanden en een jaarlijkse gegevensbeschermingsimpactanalyse.

Het RCP beschikt over 25 voltijdse medewerkers en een budget van 3,8 miljoen euro.

Er wordt nauw samengewerkt met de banksector. Elke bank heeft een RCP-*liaison officer* die zorgt voor het naleven van de rapporteringsplicht en die de contacten verzorgt met de ACD. De sector, meer bepaald de *Association des banques et banquiers, Luxembourg* (ABBL) zit regelmatig samen met de ACD en de CNPD om problemen te bespreken.

Voorts worden interne audits uitgevoerd door de ACD. Er zijn ook technische en privacy-audits. Het Luxemburgse Rekenhof mag op elk moment een inspectie uitvoeren, met speciale aandacht voor de proportionaliteit van de uitgaven en het gebruik van de middelen.

In 2024 werden geen ernstige inbreuken vastgesteld.

Wat internationale interoperabiliteit betreft, herhaalt de heer Van Quickenborne dat Luxemburg aangesloten is op BARIS. Dat systeem verbindt de nationale rekeningregisters van alle EU-lidstaten via een beveiligd netwerk. Luxemburg past hierbij het principe van de *read-only interoperability* toe. Buitenlandse autoriteiten kunnen geen directe queries uitvoeren. Verzoeken lopen via

affichés. Chaque recherche est validée au préalable par un contrôle automatique des droits. Le système vérifie si l'utilisateur dispose d'un numéro de dossier actif dans le système judiciaire ou fiscal. Chaque requête (fructueuse ou pas) est enregistrée avec plusieurs données. Ces journaux de connexion sont conservés pendant une longue période (plus de six mois). Sur les 15.000 consultations enregistrées en 2024, 60 % provenaient de l'administration fiscale, 25 % de la CRF et 15 % des autorités judiciaires.

Le RCP dispose de plusieurs niveaux de sécurité: sécurité du réseau, authentification, chiffrement et piste d'audit. La gestion des clés est assurée par la Banque centrale luxembourgeoise. L'ACD ne dispose que de clés temporaires pour le chiffrement des sessions. Ce modèle empêche qu'une seule instance ait un accès complet à toutes les données. Le système repose ensuite sur les principes de la protection de la vie privée dès la conception (*privacy by design*). Les mises en œuvre concrètes de ces principes se traduisent par des champs de données minimalistes, la suppression automatique des enregistrements inactifs, la pseudonymisation des fichiers journaux et une analyse annuelle de l'incidence sur la protection des données.

Le RCP dispose de 25 collaborateurs à temps plein et d'un budget de 3,8 millions d'euros.

Il travaille en étroite collaboration avec le secteur bancaire. Chaque banque a un officier de liaison RCP qui veille au respect de l'obligation de déclaration et assure les contacts avec l'ACD. Le secteur, plus précisément l'Association des banques et banquiers du Luxembourg (ABBL), se réunit régulièrement avec l'ACD et la CNPD pour discuter des problèmes.

En outre, des audits internes sont effectués par l'ACD. Des audits techniques et des audits de confidentialité sont également réalisés. La Cour des comptes du Grand-Duché de Luxembourg peut effectuer, à tout moment, une inspection accordant une attention particulière à la proportionnalité des dépenses et à l'utilisation des ressources.

En 2024, aucune infraction grave n'a été constatée.

En ce qui concerne l'interopérabilité internationale, M. Van Quickenborne rappelle que le Luxembourg est connecté au système BARIS, qui assure l'interconnexion entre les registres nationaux des comptes bancaires de tous les États membres de l'Union européenne par l'intermédiaire d'un réseau sécurisé. Le Luxembourg applique en l'espèce le principe de l'*interopérabilité*

de ACD, die ze handmatig goedkeurt. Loggingcontrole verloopt op Luxemburgs niveau.

Luxemburg neemt verder ook deel aan de CRS en maakt, net zoals onze CFI, deel uit van de Egmont-groep. Informatie die via het RCP wordt verkregen kan, onder de binnen de Egmont-groep geldende voorwaarden, gedeeld worden met buitenlandse tegenhangers.

Innovatie en modernisering zijn geen loze begrippen bij het RCP. Zo is er het programma *Digital Finance Integrity Luxembourg* (DFIIL) 2024-2028. Een van de pijlers is de modernisering van het RCP met een nieuwe API-architectuur en een sneller real-time validatiesysteem. Daarnaast is er het pilootproject *Predictive Maintenance*, waarbij een AI-algoritme technische storingen of onnauwkeurige uploads detecteert. Dat is meteen de enige AI-toepassing in het systeem, dat bovendien niet de data zelf, maar enkel de technische laag betreft. De CNPD heeft bevestigd dat dit niet valt onder het verbod van datamining, omdat het geen persoonlijke gegevens verwerkt.

De plannen voor 2026 hebben onder meer betrekking op de integratie van het UBO-register, een nieuwe gebruikersinterface en de uitbreiding van de CNPD-controle naar semi-automatiseerde rapporten. Er wordt ook gewerkt aan automatische notificaties aan de CNPD bij ongebruikelijke raadplegingspatronen, alsook aan een nieuwe API-laag voor snellere queries.

De (derde) tussentijdse conclusie, aldus het lid, is dat Luxemburg technologische moderniteit combineert met juridische zelfbeheersing. Het land kiest voor het model van *controlled transparency*, waar efficiëntie hand in hand gaat met de bescherming van de persoonlijke levenssfeer.

Vervolgens gaat de heer Van Quickenborne nader in op de operationele werkprocessen van het RCP. Elke werkdag voor 14 uur dienen Luxemburgse financiële instellingen hun updates in via het portaal. Het platform verwerkt de inkomende bestanden volgens een bepaalde sequentie: verificatie van de afzender, automatische validatie van structuur en consistentie, opslag in de buffer-database en migratie naar de *core database*. Het volledige proces verloopt geautomatiseerd, maar onder menselijke controle. Elke wijziging wordt meteen opgeslagen op de backup-server in Contern. De ACD voert dagelijks een *data-integrity-check* uit met een steekproef van 0,5 % van de records. Eventuele

en lecture seule. Les autorités étrangères ne peuvent effectuer aucune requête directe. Les demandes passent par l'ACD, qui les approuve manuellement. Le contrôle des connexions est assuré par le Luxembourg.

Le Luxembourg participe également au CRS et fait partie, comme notre CTIF, du groupe Egmont. Les informations obtenues par l'intermédiaire du RCP peuvent être partagées avec des homologues étrangers conformément aux conditions en vigueur au sein du groupe Egmont.

L'innovation et la modernisation ne sont pas des concepts dénués de sens au RCP. Il applique, par exemple, le programme *Digital Finance Integrity Luxembourg* (DFIIL) 2024-2028. L'un de ses piliers est la modernisation du RCP au travers d'une nouvelle architecture API et d'un système accéléré de validation en temps réel. Le RCP mène également un projet pilote dénommé "*Predictive Maintenance*", dans le cadre duquel un algorithme IA détecte les problèmes techniques ou les uploads inexacts. Il s'agit de la seule application IA de ce système, qui ne porte d'ailleurs pas sur les données en tant que telles, mais seulement sur le volet technique. La CNPD a confirmé que ce projet n'était pas visé par l'interdiction d'exploration des données, car il ne traite aucune donnée à caractère personnel.

Les projets pour l'année 2026 concernent notamment l'intégration du registre UBO, une nouvelle interface utilisateur et l'extension du contrôle de la CNPD aux rapports semi-automatisés. Des notifications automatiques à la CNPD en cas de modèles de consultation inhabituels sont également en cours d'élaboration, ainsi qu'une nouvelle couche API en vue d'accélérer les requêtes.

La (troisième) conclusion intermédiaire, selon l'intervenant, c'est que le Luxembourg allie modernité technologique et maîtrise juridique. Il a opté pour le modèle de la transparence contrôlée, dans lequel l'efficacité va de pair avec la protection de la vie privée.

M. Van Quickenborne examine ensuite plus en profondeur les processus opérationnels du RCP. Chaque jour ouvrable, avant 14 heures, les établissements financiers luxembourgeois soumettent leurs mises à jour sur le portail. La plateforme traite les fichiers entrants selon une séquence déterminée: vérification de l'expéditeur, validation automatique de la structure et de la cohérence, sauvegarde dans la base de données tampon et migration vers la *banque de données centrale*. Tout ce processus est automatisé, mais il est contrôlé par des humains. Chaque modification est immédiatement enregistrée sur le serveur de sauvegarde à Contern. L'ACD effectue quotidiennement un contrôle d'intégrité

afwijkingen worden binnen 24 uur teruggekoppeld aan de betreffende instelling.

Wanneer een bevoegde autoriteit een aanvraag indient, moeten er verschillende stappen worden gezet. Vooreerst dient er een verificatie van de aanvrager en de juridische grond plaats te vinden. Vervolgens wordt een *unique access token* (UAT) gegenereerd. Daarna volgen nog de zoekopdracht in de *core database*, de rapportage via de beveiligde interface, en de automatische logging in de audit-database. De doorlooptijd is ongeveer 38 seconden. Elke ACD-analist werkt onder supervisie van een datasteward die toeziet op rechtmatigheid en proportionaliteit. Geen enkele raadpleging mag worden uitgevoerd zonder geautoriseerde dossiercode.

Op het vlak van risicobeheersing en -beoordeling hanteert men in Luxemburg een risicogebaseerde benadering bij de toewijzing van menselijke middelen. Aanvragen worden onderverdeeld in drie categorieën. Terrorisme- en ernstige witwasdossiers krijgen hoge prioriteit. Fiscale onderzoeken van meer dan 100.000 euro hebben een gemiddelde prioriteit. Administratieve opvragingen en internationale verzoeken hebben een lage prioriteit. De indeling bepaalt enkel de volgorde van behandeling, maar niet de inhoud van de zoekactie. Als een aanvraag binnenkomt, wordt ze beoordeeld door twee analisten (vierogenprincipe). Er vindt geen automatische beslissingsondersteuning plaats.

De CNPD heeft toegang tot de querylogs en kan bepalen of bepaalde gebruikers te frequente opvragingen doen. In voorkomend geval kan een waarschuwing of een tijdelijke toegangsbeperking worden opgelegd.

Wat rapportering betreft, bezorgt de ACD halfjaarlijks een samenvattend rapport aan de desbetreffende raad met de volgende indicatoren: aantal raadplegingen, gemiddelde responstijd, foutmeldingen en gevallen van onrechtmatige toegang.

Met betrekking tot samenwerking met de banksector vermeldde de heer Van Quickenborne reeds de RCP-*liaison officers*. Banken moeten de ACD binnen de 24 uur informeren over wijzingen in de rekeninginformatie. Bij fouten of achterstand kan een administratieve boete worden opgelegd. De rapportering is volledig geautomatiseerd.

De ACD, de CNPD en de ABBL komen driemaandelijks samen in het *Comité mixte RCP*. Daarin worden onder andere de kwaliteitsnormen, de technische incidenten en de juridische vraagstukken besproken. Dat forum

des données sur un échantillon de 0,5 % des enregistrements. Les anomalies éventuelles sont signalées à l'établissement concerné dans les 24 heures.

Lorsqu'une autorité compétente introduit une demande, plusieurs démarches doivent avoir lieu. Il faut d'abord vérifier l'identité du demandeur et le fondement juridique. Un jeton d'accès unique (*unique access token*, UAT) est ensuite généré, puis viennent la recherche dans la banque de données centrale, le rapport sur l'interface sécurisée et l'enregistrement automatique dans la banque de données d'audit. Le délai d'exécution est de près de 38 secondes. Chaque analyste ACD travaille sous la supervision d'un gestionnaire de données (*data steward*) qui veille à la légalité et à la proportionnalité. Aucune consultation ne peut avoir lieu sans code de dossier autorisé.

En matière de gestion et d'évaluation des risques, le Luxembourg applique une approche fondée sur les risques pour l'affectation des ressources humaines. Les demandes sont classées en trois catégories. Une priorité élevée est accordée aux dossiers de terrorisme et d'opérations graves de blanchiment. Les enquêtes fiscales concernant des montants de plus de 100.000 euros ont une priorité moyenne. Les demandes administratives et les demandes internationales ont une priorité faible. Cette classification influence seulement l'ordre de traitement, mais pas le contenu de la recherche. Lorsqu'une demande arrive, elle est évaluée par deux analystes (principe du double contrôle). Le processus de décision ne s'appuie sur aucune aide automatisée.

La CNPD a accès aux journaux de requêtes et peut déterminer si certains utilisateurs effectuent trop souvent des requêtes. Le cas échéant, un avertissement ou une restriction temporaire d'accès peuvent être infligés.

En ce qui concerne les rapports, l'ACD fournit tous les six mois, au conseil concerné, un rapport de synthèse incluant les indicateurs suivants: nombre de consultations, temps de réponse moyen, messages d'erreur et cas d'accès illégal.

S'agissant de la collaboration avec le secteur bancaire, M. Van Quickenborne a déjà mentionné les agents de liaison RCP. Les banques doivent informer l'ACD de toute modification des informations relatives aux comptes dans les 24 heures. En cas d'erreur ou de retard, une amende administrative peut être infligée. Le rapportage est entièrement automatisé.

L'ACD, la CNPD et l'ABBL se réunissent tous les trois mois au sein du Comité mixte RCP, qui examine notamment les normes de qualité, les incidents techniques et les questions juridiques. Ce comité a un effet de

heeft een de-escalerend effect gehad, want mogelijke conflicten tussen privacy en compliance worden voortijdig beslecht.

Banken hebben geen toegang tot het register; ze zien enkel hun eigen aanleveringen. Dit is een bewuste keuze, om concurrentiegevoelige informatie te beschermen en centrale data-aggregatie door de private sector te voorkomen.

Op het vlak van de internationale samenwerking deelt Luxemburg de identificatie-informatie via BARIS met alle EU-lidstaten die over een vergelijkbaar register beschikken. Elke query van een ander lidstaat wordt manueel goedgekeurd door de ACD. Er is geen volledige geautomatiseerde datastroom.

De FATF-evaluatie van 2022 en de beoordeling door de OESO in 2023 waren positief. Beide rapporten benadrukken het sterke toezicht, de lage foutenmarge en de duidelijke grenzen voor gegevensgebruik. Wel werd aanbevolen om de technische interoperabiliteit met de CRS-systemen te versterken.

In 2024 ontving de ACD 3200 verzoeken van buitenlandse autoriteiten om bepaalde gegevens te delen. In 92 % van de gevallen werd binnen zeven dagen geantwoord. Er werden geen klachten geregistreerd over vertraging of onrechtmatige toegang.

De impact van het RCP op witwas- en fiscale onderzoeken blijkt niet gering. Volgens de CRF werden ongeveer 40 % van alle witwaszaken ondersteund door informatie uit het RCP. De fiscale administratie heeft gerapporteerd dat het register het mogelijk heeft gemaakt ongeveer 1500 belastingdossiers versneld te behandelen.

De vaakst genoemde beperkingen betreffen het ontbreken van een real-time koppeling met het UBO-register, het gebrek aan datamining voor systemische risicoanalyse en de lichte vertraging bij multinationale verzoeken via BARIS. Volgens de Europese Commissie vloeien deze evenwel voort uit bewuste beleidskeuzes, en betreft het geen echte tekortkomingen.

De kosten voor onderhoud en ontwikkeling van het RCP worden voor ongeveer 80 % gedekt door de Staat en voor een vijfde door een beperkte jaarlijkse heffing op de financiële instelling. Kan de vice-eersteminister overigens bevestigen dat het CAP wordt gefinancierd door de informatierechtigden?

désamorçage dans la mesure où il permet de résoudre à un stade précoce les conflits potentiels entre la protection de la vie privée et la conformité.

Les banques n'ont pas accès au registre, elles ne voient que leurs propres contributions. Il s'agit d'un choix délibéré, pour protéger les informations sensibles sur le plan concurrentiel et empêcher l'agrégation centralisée des données par le secteur privé.

En matière de coopération internationale, le Luxembourg partage les informations d'identification via BARIS avec tous les États membres de l'Union européenne qui disposent d'un registre similaire. Chaque requête d'un autre État membre est approuvée manuellement par l'ACD. Il n'y a pas de flux de données entièrement automatisé.

L'évaluation réalisée par le GAFI en 2022 et celle réalisée par l'OCDE en 2023 étaient positives. Les deux rapports soulignent le contrôle rigoureux, la faible marge d'erreur et les limites claires fixées à l'utilisation des données. Ils recommandaient toutefois de renforcer l'interopérabilité technique avec les systèmes relatifs au CRS.

En 2024, l'ACD a reçu 3.200 demandes de partage de certaines données émanant d'autorités étrangères. Dans 92 % des cas, une réponse a été fournie dans les sept jours. Aucune plainte n'a été enregistrée concernant des retards ou des accès illicites.

L'incidence du RCP sur les enquêtes en matière de blanchiment d'argent et de fiscalité n'est pas mince. En effet, selon la CRF, environ 40 % de toutes les affaires de blanchiment d'argent ont été étayées par des informations provenant du RCP. L'administration fiscale a indiqué que ce registre avait permis d'accélérer le traitement d'environ 1.500 dossiers fiscaux.

Les limitations les plus fréquemment mentionnées concernent l'absence de connexion en temps réel avec le registre UBO, l'absence de recours au *data mining* pour l'analyse des risques systémiques et le léger retard dans le traitement des demandes multinationales via BARIS. Selon la Commission européenne, ces limitations découlent toutefois de choix politiques délibérés et ne constituent pas de véritables dysfonctionnements.

Les frais de maintenance et de développement du RCP sont couverts à environ 80 % par l'État, et à 20 % par une taxe annuelle restreinte prélevée sur les institutions financières. Le vice-premier ministre pourrait-il par ailleurs confirmer que le PCC est financé par les personnes habilitées à recevoir à l'information?

Luxemburg werkt ook mee aan de nieuwe *European Anti-Money Laundering Authority* (AMLA).

De invoering van het RCP in 2016 betekende een fundamentele verschuiving van selectieve informatie-uitwisseling naar gecontroleerde transparantie. Het systeem is niet ontworpen als massaal surveillancemiddel, maar als een juridisch verfijnd identificatie-instrument dat de overheid in staat stelt om witwassen en belastingfraude efficiënt te bestrijden binnen een strikt privacykader. De effectiviteit van het Luxemburgse systeem staat als een paal boven water.

Het systeem kan puike operationele prestaties voorleggen. De combinatie van dagelijkse dataverversing, snelle raadpleging en minimale foutenmarge zorgt dat het RCP zeer performant is. Volgens de ACD-jaarverslagen is de verwerkingstijd tussen 2018 en 2024 gedaald van 48 uur naar minder dan één minuut.

De foutenmarge van de financiële instellingen ligt structureel onder de 0,1 %. De ACD kon via het register verschillende onverklaarde rekeningen identificeren, wat leidde tot aanvullende belastingheffing.

De belangrijkste toegevoegde waarde van het RCP ligt in de traceerbaarheid. Voor 2016 moesten de autoriteiten tientallen individuele bankbevragingen uitvoeren. Vandaag volstaat één geauthentificeerde zoekopdracht. De tijdswinst vertaalt zich in een hogere pakkans en een groter afschrikkend effect. Doordat de kwaliteit van witwasonderzoeken is gestegen kunnen onderzoeksrechters sneller netwerkstructuren in kaart brengen.

Het RCP heeft ook geleid tot een nauwere samenwerking tussen de fiscus, de CRF en het gerecht. De ACD fungeert als een coördinatieplatform om de consistentie en rechtszekerheid van informatieverzoeken te bevorderen.

Qua typologie behoort het Luxemburgse systeem tot de hybride systemen. Het CAP is, zoals al aangegeven, een centraal register. Waar het CAP wordt beheerd door de NBB en de FOD Financiën, zit het beheer van het RCP bij de ACD. De datadekking van het CAP is ruimer: het omvat alle rekeningen, inclusief saldi, daar waar het RCP beperkt is tot identificatie en openingsdata. De toegang tot het RCP is zoals gezegd beperkt tot drie instanties en dus veel minder ruim dan die tot het CAP. Privacytoezicht op het RCP en het CAP gebeurt resp. door de CNPD en de GBA. De foutenmarge van beide registers bevindt zich ongeveer op hetzelfde niveau. Het Luxemburgse model scoort lager op analytische

Le Luxembourg participe également à la nouvelle Autorité européenne de lutte contre le blanchiment de capitaux (ALBC).

La mise en place, en 2016, du RCP a représenté un basculement fondamental d'un échange d'informations sélectif vers une transparence contrôlée. Le système n'a pas été conçu comme un outil de surveillance de masse, mais comme un instrument d'identification juridiquement sophistiqué permettant aux pouvoirs publics de lutter efficacement contre le blanchiment d'argent et la fraude fiscale dans un cadre strict de respect de la vie privée. L'efficacité du système luxembourgeois ne fait aucun doute.

Ce système affiche d'excellentes prestations opérationnelles. La mise à jour quotidienne des données conjuguée à la possibilité de consultation rapide et à une marge d'erreur minimale rend le RCP très performant. Selon les rapports annuels de l'ACD, le temps de traitement est passé, entre 2018 et 2024, de 48 heures à moins d'une minute.

La marge d'erreur des institutions financières est structurellement inférieure à 0,1 %. L'ACD a pu identifier plusieurs comptes non déclarés grâce à ce registre, ce qui a donné lieu à des impositions supplémentaires.

La principale plus-value du RCP réside dans la traçabilité. Avant 2016, les autorités devaient effectuer des dizaines de requêtes bancaires individuelles, alors qu'aujourd'hui, une seule recherche authentifiée suffit. Le gain de temps se traduit par une probabilité de détection plus élevée et un effet dissuasif plus important. Grâce à l'amélioration de la qualité des enquêtes pour blanchiment d'argent, les juges d'instruction peuvent cartographier plus rapidement les structures en réseaux.

Le RCP a aussi permis une coopération plus étroite entre le fisc, la CRF et la justice. L'ACD sert de plateforme de coordination afin de renforcer la cohérence et la sécurité juridique des demandes d'informations.

Sur le plan de la classification, le système luxembourgeois fait partie des systèmes hybrides. Comme indiqué précédemment, le PCC est un registre central. Alors que le PCC est géré par la BNB et le SPF Finances, le RCP est géré par l'ACD. La couverture des données du PCC est plus large: elle comprend tous les comptes, y compris les soldes, alors que le RCP se limite à l'identification et aux dates d'ouverture des comptes. Comme mentionné précédemment, l'accès au RCP est limité à trois instances et est donc beaucoup moins large que l'accès au PCC. Ce sont respectivement la CNPD et l'APD qui se chargent de contrôler le respect de la vie privée dans le cadre du RCP et du PCC. La marge

capaciteit, maar hoger op privacybescherming en juridische robuustheid. Het Luxemburgse systeem vertoont sterkte gelijkenissen met het Duitse en Oostenrijkse, maar onderscheidt zich door de dagelijkse updatefrequentie, waardoor de informatie actueler is.

De heer Vincent Van Quickenborne (Open Vld) zet zijn vergelijking voort en focust op de sterke punten van het Luxemburgse systeem.

Ten eerste biedt dat systeem meer juridische duidelijkheid. De wet van 18 december 2015 en het reglement van 5 augustus 2016 vormen een transparant en eenduidig geheel, waarin precies wordt bepaald wie toegang heeft tot de gegevens, onder welke voorwaarden en met welke waarborgen. Ten tweede is dit systeem technologisch betrouwbaar omdat het berust op een bijzonder stabiele infrastructuur met tot nu toe geen enkel veiligheidsincident. Ten derde legt de Luxemburgse instantie een grote discipline aan de dag op het stuk van gegevensverwerking. Het vierde sterke punt van dit systeem is de internationale geloofwaardigheid ervan, dat voor meer vertrouwen zorgt van investeerders en financiële instellingen.

Luxemburg laat daarmee zien dat voor financiële transparantie niet noodzakelijk enorme hoeveelheden gegevens moeten worden verzameld. Tot slot verduidelijkt het lid dat dit systeem nauwelijks kritiek krijgt van de Luxemburgers, omdat het meer op rechtszekerheid dan op belastingcontrole gericht is.

De heer Van Quickenborne bespreekt vervolgens de zwakke punten van het Luxemburgse systeem.

Ten eerste biedt het weinig mogelijkheden voor gegevensanalyse. Bovendien verhindert het verbod op datamining de vroegtijdige opsporing van systemische risico's. De financiële inlichtingendienst (CRF) en de belastingdienst (ACD) baseren zich op externe indicatoren.

Voorts worden de gegevens weliswaar dagelijks bijgewerkt, maar is er geen realtimekoppeling met de banken. Er kan een vertraging van enkele uren bestaan tussen de daadwerkelijke transacties en de registratie ervan, wat een grote hinderpaal kan zijn bij dringende strafzaken.

Een bijkomend aspect is de complexe governance in Luxemburg. Die veronderstelt samenwerking tussen de ACD, de CNPD (toezichthouder), de CSSF (controle-commissie voor de financiële sector) en de CRF. Zulke

d'erreur des deux registres est à peu près la même. Le modèle luxembourgeois obtient un score inférieur en matière de capacité analytique, mais supérieur en matière de protection de la vie privée et de robustesse juridique. Le système luxembourgeois présente de fortes similitudes avec les systèmes allemand et autrichien, mais se distingue par la fréquence quotidienne de ses mises à jour, qui rend les informations plus actuelles.

M. Van Quickenborne (Open Vld) poursuit sa comparaison et se concentre sur les points forts du système luxembourgeois.

Tout d'abord, c'est un système qui offre davantage de clarté juridique. La loi du 18 décembre 2015 et le règlement du 5 août 2016 constituent un ensemble transparent et sans équivoque, qui définit précisément qui a accès aux données, à quelles conditions et moyennant quelles garanties. Ensuite, ce système est fiable sur le plan technologique, car il est fondé sur une infrastructure particulièrement stable qui n'a connu, jusqu'ici, aucun incident de sécurité. Troisièmement, l'instance luxembourgeoise fait preuve d'une grande discipline en matière de traitement des données. Le quatrième atout de ce système est sa crédibilité sur le plan international, qui renforce la confiance des investisseurs et des institutions financières.

Le Luxembourg démontre ainsi que la transparence financière n'implique pas nécessairement une collecte massive de données. Enfin, le membre précise que ce système est très peu critiqué par les citoyens luxembourgeois car il est axé sur la sécurité juridique plutôt que sur le contrôle fiscal.

M. Van Quickenborne s'attarde ensuite sur les faiblesses du système luxembourgeois.

Tout d'abord, il offre peu d'opportunités en matière d'analyse des données. De plus, l'interdiction de data mining empêche la détection précoce des risques systémiques. La Cellule de renseignement financier (CRF) et l'administration fiscale (ACD) s'appuient sur des indicateurs externes.

Ensuite, bien que les données soient mises à jour quotidiennement, il n'existe aucune intégration en temps réel avec les banques. Un délai de plusieurs heures peut exister entre les transactions effectives et leur enregistrement, ce qui peut constituer un obstacle majeur dans les affaires pénales urgentes.

Un autre défaut est la complexité du système de gouvernance. Il implique une collaboration entre l'ACD, la CNPD (autorité de surveillance), la CSSF (autorité de contrôle du secteur) et la CRF, qui exige une coordination

samenwerking vereist permanente coördinatie, maar een centrale coördinatieraad ontbreekt vooralsnog.

Dan is er de druk vanuit Europa. AMLA, de Europese antiwitwasautoriteit, pleit voor een uniforme Europese standaard. Doel is het systeem tegen 2027 in overeenstemming te brengen met het Europees netwerk, een uitdaging van formaat.

Er zijn ook de toekomstige digitale risico's. De toenemende digitalisering en opkomst van AI-toepassingen binnen de bankensector kunnen de minimale RCP-gegevensverwerking onder druk zetten. Het gebruik van *privacy preserving analytics* (privacybeschermende analyse), waarbij patronen kunnen worden ontwaard zonder persoonsgegevens prijs te geven, is voer voor toenemend debat. De CNPD onderzoekt thans of die technologie verenigbaar is met de Luxemburgse grondwet.

Los daarvan is de Europese Commissie van oordeel dat Luxemburg in hoge mate voldoet aan de AMLA-regelgeving. Het Luxemburgse aanspreekpunt voldoet aan de technische en juridische vereisten van die regelgeving, met uitzondering van het ontbreken van geautomatiseerde risicoprofielen. Luxemburg vervult een bijzondere rol binnen de Europese bankenunie. Het biedt internationale financiële instellingen een veilige, maar transparante omgeving. Het RCP draagt aan die reputatie bij door te fungeren als juridische schakel tussen nationale beslissingsmacht en Europese transparantie. Er wordt thans gewerkt aan een koppeling tussen het RCP en het UBO-register, in samenhang met de aanleg van dat register. De bedoeling is met cryptografische pseudonimiseringssystemen te werken, zodat identificatie enkel gebeurt door het gerecht. Die innovatie zou Luxemburg positioneren als pionier op het vlak van privacybeschermende transparantie.

Voor de spreker is de doeltreffendheid van het Luxemburgse systeem onbetwist. De zwakte ervan schuilt niet in de werking maar in de opgelegde juridische beperkingen, die voortvloeien uit een doelbewuste beleidsfilosofie. Luxemburg streeft niet naar maximale transparantie, maar naar maximale rechtszekerheid. De registers zijn strikt gereguleerd, technologisch voldragen en maatschappelijk legitiem.

Over het Luxemburgse model voor financieel toezicht kan men concluderen dat de uitdaging voor de komende jaren niet de uitbreiding van bevoegdheden is, maar het consolideren en perfectioneren van het bestaande evenwicht tussen transparantie, efficiëntie en grondrechten.

continue. Or, le Conseil central de coordination fait encore défaut.

À cela s'ajoute la pression européenne. L'Autorité européenne de lutte contre le blanchiment d'argent (ALBA) œuvre à l'élaboration d'une norme européenne uniforme. L'objectif est de rendre le système conforme au réseau européen d'ici 2027, ce qui représente un véritable défi.

Des risques numériques futurs existent également. L'essor de la numérisation et des applications d'IA dans le secteur bancaire pourrait indirectement exercer une pression sur la minimisation des données du RCP. L'utilisation d'une analyse respectueuse de la vie privée, qui permet de détecter des tendances sans révéler de données personnelles, fait l'objet d'un débat croissant. La CNPD examine actuellement la compatibilité de ces technologies avec la Constitution luxembourgeoise.

Cela étant, la Commission européenne considère le Luxembourg comme étant hautement conforme à la réglementation de l'ALBA. Le PCC luxembourgeois satisfait aux exigences techniques et juridiques de cette réglementation, à l'exception de l'absence de profils de risque automatisés. Le Luxembourg joue un rôle particulier au sein de l'Union bancaire européenne. Il offre un environnement à la fois sécurisé et transparent aux institutions financières internationales. Le RCP contribue à cette réputation en servant de lien juridique entre le pouvoir discrétionnaire national et la transparence européenne. Un lien entre le RCP et le registre des bénéficiaires effectifs (UBO) est en cours d'élaboration, en parallèle avec la création de ce dernier. L'objectif est d'utiliser des systèmes de pseudonymisation cryptographique afin que l'identification ne soit effectuée que par les autorités judiciaires. Cette innovation positionnerait le Luxembourg comme un pionnier de la transparence respectueuse de la vie privée.

Dès lors, pour le membre, l'efficacité du système luxembourgeois est incontestable. Sa faiblesse ne réside pas dans son fonctionnement, mais dans les limitations juridiques qui lui sont imposées, qui relèvent d'une philosophie politique délibérément choisie. Le Luxembourg ne privilégie pas la transparence maximale, mais la sécurité juridique maximale. Les registres sont strictement réglementés, technologiquement aboutis et socialement légitimes.

La conclusion, concernant le modèle de supervision financière luxembourgeois, est que le défi pour les années à venir n'est pas l'extension des pouvoirs, mais la consolidation et le perfectionnement de l'équilibre actuel entre transparence, efficacité et droits fondamentaux.

De heer Van Quickenborne gaat voorts in op de strategische principes van de hervorming in Luxemburg. Een eerste doelstelling is het verbeteren van de operationele doeltreffendheid door ervoor te zorgen dat ambtenaren en bevoegde overheden snel toegang krijgen tot accurate rekeninginformatie. Ten tweede is de bescherming van de individuele vrijheden van essentieel belang. Het is de bedoeling te voorkomen dat het register een instrument wordt voor massale gegevensanalyse. Die tweedeling is niet paradoxaal, maar structureel. Het RCP is gebaseerd op het principe dat beperkte toegang een garantie is voor betrouwbaarheid. Ten slotte is het Luxemburgse model gebaseerd op het principe van transparantie op verzoek. Dat onderscheidt het van de Belgische “standaardtransparantie”, zoals voorzien in het *money control*-systeem. De Luxemburgse aanpak koppelt elke raadpleging van gegevens aan een concrete en verifieerbare reden, waardoor de evenredigheid wordt gewaarborgd.

In Luxemburg bestaat er een brede consensus: geen uitbreiding van geautomatiseerde profilering, maar wel bewaring van inloggegevens en interoperabiliteit met de EU, maar zonder overdracht van bevoegdheden. De regering bereidt momenteel een herziening voor van de wet van 18 december 2015, die een reeks hervormingsvoorstellen omvat, met name:

- een verduidelijking van het verbod op geautomatiseerde gegevensanalyse;
- meer samenwerking tussen de ACD, de CNPD en de CRF;
- invoering van sancties in geval van onrechtmatige toegang door buitenlandse autoriteiten;
- realtimevalidatie zonder datamining;
- realtimeverwerking van verzoeken, waardoor informatie onmiddellijk beschikbaar is zonder dat bijkomende gegevens worden opgeslagen;
- verbetering van de koppeling tussen het RCP en het register van uiteindelijke begunstigen dankzij het gebruik van een cryptografisch pseudoniem, waardoor complexe structuren kunnen worden geanalyseerd zonder het beginsel van minimale gegevensverwerking te schenden;
- de invoering van een kwaliteits- en opleidingsprogramma;
- governance- en toezichtplannen gericht op transparantie, publieke communicatie, de publicatie van

M. Van Quickenborne aborde ensuite les principes stratégiques de la réforme au Luxembourg. Les objectifs poursuivis sont, tout d’abord, d’améliorer l’efficacité opérationnelle, en garantissant aux fonctionnaires et autorités compétents un accès rapide à des informations de compte précises. Ensuite, la protection des libertés individuelles est essentielle. Il s’agit d’empêcher que le registre ne devienne un instrument d’analyse de données de masse. Cette dichotomie n’est pas paradoxale, mais structurelle. La RCP repose sur le principe qu’un accès limité est gage de fiabilité. Enfin, le modèle luxembourgeois est fondé sur le principe de la transparence sur demande. Cela le distingue de la transparence “par défaut” belge, telle que prévue par le système de *money control*. L’approche luxembourgeoise associe chaque consultation de données à une raison concrète et vérifiable, garantissant ainsi la proportionnalité.

Au Luxembourg, un large consensus se dégage: pas d’extension du profilage automatisé, conservation des identifiants de connexion et interopérabilité avec l’UE sans transfert de compétences. Le gouvernement prépare actuellement une révision de la loi du 18 décembre 2015, comprenant une série de propositions de réforme, notamment:

- la clarification de l’interdiction de l’analyse automatisée des données;
- le renforcement de la coopération entre l’ACD, la CNPD et le CRF;
- l’introduction de sanctions en cas d’accès non autorisé par des autorités étrangères;
- la validation en temps réel sans exploration de données;
- le traitement des requêtes en temps réel, permettant une mise à disposition immédiate des informations sans stockage de données supplémentaires;
- l’amélioration du lien entre le RCP et le registre des bénéficiaires effectifs, grâce à l’utilisation d’un pseudonyme cryptographique, permettant l’analyse de structures complexes sans enfreindre le principe de minimisation des données;
- la mise en place d’un programme de qualité et de formation;
- des plans de gouvernance et de contrôle axés sur la transparence, la communication publique, la publication

het jaarverslag, van statistieken en van auditverslagen, alsook een follow-up van incidenten;

- versterking van de CNPD;
- toegang van de CNPD tot de auditlogboeken voor een permanent toezicht op het rekeningregister;
- digitale innovatie en bestendigheid van de systemen;
- privacyvriendelijke analyses;
- verder onderzoek naar differentiële privacy en specifieke versleuteling, alsook naar cyberveiligheid en veerkracht.

De regering erkent dat AI de komende jaren een almaar belangrijkere rol zal spelen in de strijd tegen het witwassen van geld, maar heeft niettemin gekozen voor een AI-model onder toezicht. Dat betekent dat de algoritmen technische schema's opsporen, zoals dubbele downloads, maar geen gedragsanalyse kunnen uitvoeren of niet aan individuele risicoprofilering kunnen doen. De CNPD en de ACD werken samen aan de ontwikkeling van wettelijke regels voor AI, ethiek en systemen voor financiële gegevens.

Wat zijn de economische en institutionele gevolgen van het Luxemburgse systeem voor de financiële sector? De banksector ziet het RCP niet langer als een beperking, maar als een waarborg voor rechtszekerheid. De automatische aangifte is niet duur (minder dan 0,02 euro per registratie). De banken genieten hierdoor een reputatievoordeel. Door mee te werken aan een streng maar rechtvaardig systeem versterken ze hun geloofwaardigheid bij hun internationale partners. Het systeem consolideert de rechtsstaat. Het garandeert de doeltreffendheid van het gerecht zonder de individuele vrijheden aan te tasten. Het is een schoolvoorbeeld van technologische evenredigheid en digitale infrastructuur die de staat versterkt zonder de burgers te verzwakken.

Het systeem beïnvloedt ook de internationale positie van Luxemburg, dat binnen de Financial Action Task Force (FATF) als een model voor gegevensbescherming wordt gezien. Onder andere Ierland heeft zijn aanpak geënt op die van Luxemburg. Die diplomatieke invloed draagt bij aan de economische positie van Luxemburg als stabiel financieel centrum binnen de EU.

Tot slot somt het lid een aantal beleidsaanbevelingen op:

du rapport annuel, des statistiques, des rapports d'audit et le suivi des incidents;

- le renforcement de la CNPD;
- l'octroi à la CNPD d'un accès aux journaux d'audit pour une surveillance continue du registre des comptes;
- l'innovation numérique et la pérennisation des systèmes;
- des analyses respectueuses de la vie privée.
- la poursuite de recherches sur la confidentialité différentielle et le chiffrement spécifique, ainsi que sur la cybersécurité et la résilience.

Le gouvernement reconnaît que l'IA jouera un rôle de plus en plus important dans la lutte contre le blanchiment d'argent dans les années à venir, mais a opté pour un modèle d'IA supervisée. Cela signifie que les algorithmes détectent les schémas techniques, tels que les téléchargements en double, mais ne peuvent pas effectuer d'analyse comportementale ni de profilage des risques individuels. La CNPD et l'ACD collaborent à l'élaboration de cadres juridiques pour l'IA, l'éthique et les systèmes de données financières.

Quel est l'impact économique et institutionnel du système luxembourgeois sur le secteur financier? Le secteur bancaire ne perçoit plus le RCP comme une contrainte, mais comme une garantie de sécurité juridique. La déclaration automatique est peu coûteuse (moins de 0,02 euro par enregistrement). Les banques bénéficient d'un avantage en termes de réputation. En participant à un système rigoureux mais équitable, elles renforcent leur crédibilité auprès de leurs partenaires internationaux. Le système consolide l'état de droit. Il garantit l'efficacité de la justice sans porter atteinte aux libertés individuelles. Il constitue un exemple type de proportionnalité technologique et d'infrastructure numérique qui renforce l'État sans affaiblir les citoyens.

Ce système influence également la position internationale du Luxembourg, qui se présente dans le cadre du GAFI comme un modèle de protection des données. L'Irlande, entre autres, a calqué son approche sur celle du Luxembourg. Cette influence diplomatique contribue à la position économique du Luxembourg en tant que place financière stable au sein de l'UE.

Enfin, le membre énumère plusieurs recommandations politiques qui peuvent être formulées:

1. formele opname in een codex;
2. oprichting van een permanente coördinatieraad;
3. toegang onder toezicht in realtime;
4. interactie met het register van uiteindelijke begunstigen (UBO);
5. transparant toezicht;
6. ethische kaders voor AI;
7. openbare communicatie;
8. Europese interoperabiliteit;
9. een onafhankelijke evaluatie en een financieringsregeling, waarbij publieke middelen worden gevrijwaard en tegelijk aangevuld met een onderhoudsbijdrage van de banken.

Luxemburg heeft gekozen voor een juridisch evenwicht dat uniek is in Europa. Terwijl veel landen de voorkeur geven aan centralisatie en algoritmische analyse, laat Luxemburg zien dat toegangscontrole en een betere bescherming van de persoonlijke levenssfeer niet onverenigbaar zijn met efficiëntie. Dat systeem is gebaseerd op drie pijlers:

- juridische duidelijkheid: nauwkeurige wetgeving en strikte scheiding der machten;
- technologische betrouwbaarheid: een moderne infrastructuur met volledige controlemogelijkheden;
- democratische verantwoordelijkheid dankzij onafhankelijk toezicht en parlementaire verslagen.

Dit systeem blijft een referentie in Europa voor de manier waarop technologie, de rechtsstaat en vertrouwen elkaar kunnen versterken.

Vervolgens beschrijft de heer Van Quickenborne het systeem dat in de Europese Unie van kracht is.

Hij herinnert eraan dat de manier waarop gegevens binnen de EU worden verwerkt, alsook de impact ervan en de flankerende regels ter zake, onlosmakelijk verbonden zijn met de regels aangaande de bescherming van de persoonsgegevens, waarnaar de EU-lidstaten zich dienen te schikken. Dat heeft grote gevolgen op het vrij verkeer van kapitaal en van personen. Als kapitaal vrij mag circuleren, moeten gegevens dat ook kunnen. Informatie en gegevens vormen de nieuwe vertrouwensbasis. Ze maken deel uit van een breder Europees

1. codification formelle;
2. création d'un conseil de coordination permanent;
3. accès supervisé en temps réel;
4. interaction avec le registre des bénéficiaires effectifs (UBO);
5. supervision transparente;
6. cadres éthiques pour l'IA;
7. communication publique;
8. interoperabilité européenne.
9. Évaluation indépendante et mécanisme de financement préservant les fonds publics tout en les complétant par une contribution des banques pour la maintenance.

Le Luxembourg a opté pour un équilibre juridique unique en Europe. Alors que de nombreux pays privilégient la centralisation et l'analyse algorithmique, le Luxembourg démontre que le contrôle d'accès et une protection renforcée de la vie privée ne sont pas incompatibles avec l'efficacité. Ce système repose sur trois piliers:

- clarté juridique: une législation précise et une séparation stricte des pouvoirs;
- fiabilité technologique: une infrastructure moderne avec des pistes d'audit complètes;
- responsabilité démocratique grâce à un contrôle indépendant et à des rapports parlementaires.

Ce système demeure une référence en Europe quant à la manière dont la technologie, l'état de droit et la confiance peuvent se renforcer mutuellement.

M. Van Quickenborne s'attelle ensuite à décrire le système en vigueur au sein de l'Union européenne (UE).

Il rappelle qu'au sein de l'UE, la manière dont sont traitées les données, leur impact et les règles qui les encadrent sont indissociables des règles de protection des données personnelles, auxquelles les États membres de l'UE sont tenus de se conformer. Cela a des implications majeures sur la liberté des capitaux et la libre circulation des personnes. Si les capitaux peuvent circuler, les données doivent pouvoir en faire autant. L'information et les données constituent le nouveau fondement de la confiance. Elles s'inscrivent dans un

kader waarin nationale registers onderling gekoppeld en gestandaardiseerd zijn en kunnen worden vergeleken.

Sinds de financiële crisis van 2008 maakt de Europese Commissie werk van de oprichting van een gemeenschappelijke ruimte voor financiële gegevens, met als doel dankzij de uitwisseling van informatie tussen de lidstaten witwaspraktijken, belastingfraude en de financiering van terrorisme te bestrijden. Bij een niet-optimale gegevensuitwisseling zou het goed kunnen dat een terrorist die zich van punt A naar punt B verplaatst, van de radar verdwijnt. Hetzelfde geldt voor betalingsstromen. Witwaspraktijken vinden bijna altijd buiten de landsgrenzen plaats. Vandaar het belang van een doeltreffende gegevensuitwisseling om ze te bestrijden.

De digitale infrastructuur van de lidstaten, zoals het Belgische CAP, vormen dus de structuur van die Europese dataruimte. De tenuitvoerlegging ervan wordt gewaarborgd door de antiwitwasrichtlijnen (*anti-money laundering directives* – AMLD), die later zijn aangenomen.

Volgens de heer Van Quickenborne is de belangrijkste richtlijn in dat verband de vierde, in 2015 aangenomen antiwitwasrichtlijn, die elke lidstaat verplicht een centraal register van bankrekeningen op te zetten. Dit is de bestaansreden van het Belgische CAP, waarmee dus aan een Europese verplichting wordt voldaan, hoewel het CAP al sinds 2011 bestaat. Sinds 2015 en het aannemen van de AMLD-4 overstijgt het gebruik ervan evenwel het nationale kader: het maakt het deel uit van een Europees netwerk en dient aan uniforme technische vereisten te voldoen.

De heer Van Quickenborne wijst er verder op dat in de loop der jaren vijf AMLD's werden opgesteld. De eerste antiwitwasrichtlijn dateert uit 1991. In 2001, in de nasleep van de aanslagen van 11 september, werd de AMLD-2 aangenomen, teneinde het toepassingsgebied tot de financiering van het terrorisme uit te breiden. De derde antiwitwasrichtlijn (AMLD-3) uit 2005 breidde het toepassingsgebied uit tot niet-financiële beroepen. Met de vierde richtlijn, de AMLD-4, werd het centraal rekeningenregister ingevoerd. Vervolgens focuste de AMLD-5-richtlijn van 2018 op de transparantie inzake de *ultimate beneficial owners* (UBO) en de digitale identificatie, dus op de identificatie van de aandeelhouders van een bedrijf. Tot slot hebben de zesde richtlijn, de AMLD-6, en de nieuwe AMLA-verordening uit 2024 het toezicht op Europees niveau versterkt.

De rol van de Europese Commissie bestaat erin erop toe te zien dat die richtlijnen worden omgezet. De Europese Commissie kan bij inbreuken tevens gerechtelijke stappen ondernemen. De heer Van Quickenborne wijst erop dat België felicitaties heeft ontvangen voor

cadre européen plus large, où les registres nationaux sont interconnectés, normalisés et comparés.

Depuis la crise financière de 2008, la Commission européenne travaille à la mise en place d'un espace commun de données financières. L'objectif est de lutter contre le blanchiment d'argent, la fraude fiscale et le financement du terrorisme grâce à l'échange d'informations entre les États membres. Si cet échange d'informations n'est pas optimisé, un terroriste qui se déplace d'un point à un autre risque de devenir introuvable. Il en va de même pour les flux de paiements. Le blanchiment d'argent est un phénomène qui se produit presque toujours au-delà des frontières nationales. Un échange d'informations efficace est donc indispensable pour le combattre.

Les infrastructures numériques des États membres, telle que le PCC belge, constitue donc la structure de cet espace européen de données. Sa mise en œuvre est assurée par des directives anti-blanchiment (Anti-Money Laundering Directive – AMLD), adoptées ultérieurement.

Selon le membre, la plus importante dans ce contexte est la 4^e directive AMLD, adoptée en 2015, qui oblige chaque État membre à établir un registre central des comptes bancaires. C'est la raison d'être du PCC belge, qui relève donc d'une obligation européenne. Cependant, le PCC belge existait déjà en 2011. Mais depuis 2015 et l'AMLD-4, il n'est plus isolé dans un cadre national, mais fait partie d'un réseau européen, avec des exigences techniques uniformes.

M. Van Quickenborne rappelle ensuite que cinq directives AMLD ont été élaborées au fil des ans. La première directive AMLD date de 1991. En 2001 a été adoptée la directive AMLD-2, suite aux attentats du 11 septembre, pour élargir le champ d'application au financement du terrorisme. La troisième directive anti-blanchiment (AMLD-3) de 2005 a étendu le champ d'application aux professions non financières. La quatrième, l'AMLD-4, a instauré le Registre central des comptes (RCC). Puis, en 2018, l'AMLD-5 a porté sur la transparence des bénéficiaires effectifs (UBO) et l'identification numérique, c'est-à-dire l'identification des actionnaires d'une société. Enfin, la sixième directive, l'AMLD-6, ainsi que le nouveau règlement AMLA de 2024, ont renforcé la supervision au niveau européen.

Le rôle de la Commission européenne est de superviser la transposition de ces directives. Elle peut également engager des poursuites en cas d'infraction. Le membre souligne que la Belgique a été félicitée pour la mise en œuvre rapide de l'AMLD-5 en 2020. Notre

de snelle omzetting van de AMLD-5 in 2020. Ons land is dan ook klaar om de AMLD-5, en meer specifiek het UBO-register, zo snel mogelijk ten uitvoer te leggen.

Wat de Europese Centrale Bank (ECB) betreft, meent de spreker dat ze geen rechtstreekse bevoegdheid heeft, in ieder geval niet inzake het bestrijden van witwaspraktijken. Zij ziet echter toe op de naleving van de aangifteverplichtingen via haar *single supervisory mechanism* (SSM). De ECB verwacht ook van de banken dat ze hun interne systemen met de nationale registers in lijn brengen, teneinde de samenhang bij de identificatie van de klanten (KYC – *know your client*) te waarborgen. Door met de nationale centrale banken, zoals de Nationale Bank van België, samen te werken, wordt technische convergentie mogelijk, zoals het gebruik van identieke gegevensformaten, beveiligingsprotocollen en authenticatiestructuren. Die samenwerking komt het CAP ten goede doordat het aldus toegang krijgt tot expertise op het vlak van de veiligheid van de financiële gegevens.

De heer Van Quickenborne verwijst vervolgens naar het advies dat aan de Raad van State werd gevraagd. In dat advies staat dat ook de Nationale Bank, de Inspectie van Financiën en zelfs de Europese Centrale Bank advies dienen te geven. De huidige regering heeft het advies van die instellingen niet ingewonnen, wat op lange termijn problematisch zou kunnen uitdraaien. Indien voor een rechtbank wordt vastgesteld dat het desbetreffende advies niet werd gevraagd, zal de tolerantie zeer klein zijn.

De heer Van Quickenborne merkt bovendien op dat de antiwitwaswetgeving momenteel evolueert van richtlijnen naar verordeningen. In tegenstelling tot een verordening evolueert een richtlijn echter van coördinatie naar integratie. Dat brengt het toezicht dicht bij de Europese instelling, terwijl de nationale parlementen middelen moeten vinden om hun democratische controle te behouden. Kortom, het hele systeem, de spanning tussen richtlijnen, verordeningen, toezicht, controle en organisatie, vormt de essentie van de strijd tegen witwaspraktijken.

Het lid wijst er voorts op dat België volgens een recent rapport een van de drie landen is met de meest geavanceerde architectuur. Daar zouden drie redenen voor zijn. Vooreerst wordt het CAP aangestuurd door een onafhankelijke entiteit, namelijk de Nationale Bank van België, en is het binnen de structuur ervan geïntegreerd. Ten tweede heeft België een juridisch bindend kwaliteitscontrolesysteem. Ten derde voldoet het auditmechanisme van ons land aan de Europese normen. De Europese Commissie bestempelt deze situatie als institutionele neutraliteit, omdat de beheerder geen direct

pays est donc prêt à mettre en œuvre l'AMLD-5, et plus particulièrement le registre des bénéficiaires effectifs, dans les meilleurs délais.

Pour ce qui est de la Banque centrale européenne (BCE), le membre pense qu'elle ne dispose pas d'une autorité directe, du moins en matière de lutte contre le blanchiment d'argent. Cependant, elle contrôle le respect des obligations de déclaration par le biais de son mécanisme de surveillance unique (MSU). La BCE attend également des banques qu'elles harmonisent leurs systèmes internes avec les registres nationaux afin de garantir la cohérence de l'identification des clients (KYC – *Know your Client*). La collaboration avec les banques centrales nationales, comme la Banque nationale de Belgique, permet une convergence technique, c'est-à-dire l'utilisation de formats de données, de protocoles de sécurité et de structures d'authentification identiques. Le PCC bénéficie de cette collaboration en donnant accès à une expertise en matière de sécurité des données financières.

Le membre fait ensuite référence à l'avis sollicité auprès du Conseil d'État. Cet avis stipule que la Banque nationale, l'Inspection financière et même la Banque centrale européenne devraient aussi donner leur avis. Le gouvernement actuel n'a pas sollicité l'avis de ces institutions, ce qui pourrait s'avérer problématique à long terme. S'il est établi devant un tribunal que cet avis n'a pas été sollicité, la marge de tolérance sera très réduite.

Par ailleurs, M. Van Quickenborne observe qu'il y a actuellement une évolution de la législation anti-blanchiment, des directives aux règlements. Or contrairement à un règlement, une directive évolue de la coordination à l'intégration. Cela rapproche la supervision de l'institution européenne, tandis que les parlements nationaux doivent trouver des moyens de préserver leur contrôle démocratique. En résumé, tout le dispositif, la tension entre directives, règlements, supervision, contrôle et organisation, constitue l'essence même de la lutte contre le blanchiment d'argent.

Le membre indique par ailleurs que selon un rapport récent, la Belgique figure parmi les trois pays dotés de l'architecture la plus avancée. Il y aurait trois raisons à cela. Premièrement, le PCC est piloté par une entité indépendante, la Banque nationale de Belgique, et est intégré à la structure de cette dernière. Deuxièmement, la Belgique dispose d'un contrôle qualité juridiquement contraignant. Troisièmement, son mécanisme d'audit est conforme aux normes européennes. La Commission européenne qualifie cette situation de neutralité institutionnelle, car l'administrateur n'a aucun intérêt direct dans

belang heeft bij het gebruik van de gegevens, wat het vertrouwen versterkt en misbruik voorkomt. Het CAP en de Nationale Bank halen met andere woorden geen voordeel uit de raadpleging van het CAP. De maatregelen met het oog op administratieve vereenvoudiging verplichten de overheidsdiensten ertoe het Rijksregister van de natuurlijke personen te raadplegen in plaats van de informatie op te vragen bij de burgers. Vroeger werden er echter voor elke raadpleging kosten aangerekend. Dat probleem is nu opgelost.

In vergelijking met de andere reeds eerder genoemde landen bevindt België zich tussen de gecentraliseerde modellen en het Duitse federale model, dat werkt met een onafhankelijk technisch beheer binnen een federale juridische structuur. In Frankrijk is er volledige integratie met de belastingdiensten. In België is er een onafhankelijke technische beheerder en in Duitsland bestaat er een sterke scheiding tussen de banken en de belastingdiensten.

Het lid attendeert er ook op dat België tijdens het Belgische voorzitterschap van de Raad van de Europese Unie een werkgroep heeft geleid die de overgang naar de AMLA moest voorbereiden. Ons land zou toen gehamerd hebben op het belang van een duidelijk onderscheid tussen gegevensregistratie en -analyse. Die nuance werd uiteindelijk opgenomen in de AMLA-verordening, waarbij met name werd bepaald dat de centrale registers de feitelijke gegevens verzamelen, terwijl de risicoanalyse de bevoegdheid is van afzonderlijke autoriteiten.

Het lid gaat vervolgens in op de toestand buiten de EU. Op dat niveau is het de OESO die een raamwerk oplegt, via de Common Reporting Standard (CRS).

De CRS, die in 2014 werd ingevoerd, regelt de automatische uitwisseling van inlichtingen betreffende financiële rekeningen in tientallen landen over de hele wereld, waaronder Chili en Australië. België heeft deze norm omgezet bij de wet van 16 december 2015. Het is een van de voornaamste internationale instrumenten in de strijd tegen grensoverschrijdende belastingfraude.

Deze standaard werd door de OESO opgesteld op vraag van de G20 en heeft sinds 2014 de invoering mogelijk gemaakt van een mondiale infrastructuur voor de automatische uitwisseling van informatie over financiële rekeningen tussen belastingdiensten.

De Europese DAC2-richtlijn van 2014 (2014/107/EU) werd door dezelfde wet van 2015 omgezet in Belgisch recht. De CRS-verordening en de DAC2 vormen samen het juridische raamwerk voor de automatische melding van buitenlandse rekeninghouders, waardoor het

l'utilisation des données, ce qui renforce la confiance et prévient les abus. Autrement dit, le PCC et la Banque nationale ne tirent aucun bénéfice de la consultation du PCC. Les mesures liées à la simplification administrative obligent les administrations à consulter le Registre national au lieu de demander les informations aux citoyens. Mais auparavant, chaque consultation était payante. Ce problème est maintenant résolu.

Par rapport aux autres pays déjà cités, la Belgique se situe entre les modèles centralisés et le modèle fédéral allemand, qui fonctionne avec une gestion technique indépendante au sein d'une structure juridique fédérale. En France, l'intégration avec l'administration fiscale est totale. En Belgique, il s'agit d'un gestionnaire technique indépendant, et en Allemagne, il existe une forte séparation entre les banques et l'administration fiscale.

Le membre fait également remarquer que, lors de la présidence belge du Conseil de l'Union européenne, la Belgique a piloté un groupe de travail chargé de préparer la transition vers l'AMLA. Notre pays aurait insisté, à cette occasion, sur l'importance de faire une distinction claire entre l'enregistrement et l'analyse des données. Cette nuance a finalement été intégrée au règlement AMLA, stipulant notamment que les registres centraux collectent les données factuelles, tandis que l'analyse des risques relève d'autorités distinctes.

Le membre aborde ensuite la situation en dehors de l'UE. À ce niveau, c'est l'OCDE qui impose un cadre, à travers la Norme commune de déclaration (NCD).

La NCD, instaurée en 2014, régit l'échange automatique de renseignements relatifs aux comptes financiers dans des dizaines de pays à travers le monde, dont le Chili et l'Australie. La Belgique a transposé cette norme par la loi du 16 décembre 2015. Il s'agit de l'un des instruments internationaux les plus importants dans la lutte contre la fraude fiscale transfrontalière.

Élaborée par l'OCDE à la demande du G20, cette norme a permis la mise en place, depuis 2014, d'une infrastructure mondiale pour l'échange automatique de renseignements relatifs aux comptes financiers entre les administrations fiscales.

La directive européenne DAC-2 de 2014 (2014/107/UE) a également été transposée en droit belge à travers la même loi de 2015. Le règlement NCD et la DAC-2 constituent ensemble le cadre juridique de la déclaration automatique des titulaires de comptes étrangers,

traditionele obstakel van het bankgeheim fundamenteel is weggenomen.

De heer Van Quickenborne bespreekt de redenen voor de creatie van de CRS. In de jaren 2000 werd duidelijk dat de gegevensuitwisseling tussen staten ontoereikend was om belastingfraude te bestrijden. Het bankgeheim, symbool van financiële autonomie, werd gezien als een belemmering voor een eerlijke belastingheffing in een geglobaliseerde economie. In 2009 koos de G20-top in Londen, die onmiddellijk na de financiële crisis plaatsvond, voor een nieuw tijdperk inzake transparantie. De OESO kreeg toen de opdracht een eenvormig model uit te werken voor de automatische aangifte van financiële gegevens. Na vier jaar onderhandelen werd in juli 2014 de CRS aangenomen.

Het belangrijkste doel van de CRS is een wereldwijd gestandaardiseerd mechanisme voor de automatische uitwisseling van informatie over financiële rekeningen, teneinde grensoverschrijdende belastingontwijking te voorkomen. Met andere woorden, terwijl het CAP toezicht houdt op de nationale rekeningen, zorgt de CRS voor de transnationale opsporing. Het systeem is opgenomen in het multilateraal akkoord tussen bevoegde autoriteiten betreffende de automatische uitwisseling van inlichtingen inzake financiële rekeningen (*Multilateral Competent Authority Agreement – MCAA*), dat gebaseerd is op artikel 6 van het OESO-verdrag inzake wederzijdse administratieve bijstand in belastingzaken. Dat verdrag geeft staten de bevoegdheid om informatie op verzoek uit te wisselen, spontaan te delen of automatisch te delen volgens een overeengekomen norm. België ondertekende het MCAA in 2014 en verbond zich tot de eerste automatische uitwisseling in 2017.

De CRS is niet rechtstreeks bindend, maar de toepassing ervan wordt mogelijk gemaakt door nationale wetgeving. Elke deelnemende staat moet financiële instellingen ertoe verplichten gegevens te verzamelen. Er moet worden voorzien in een wettelijk kader voor de doorgifte van gegevens aan de belastingdiensten en er moet een administratief systeem worden opgezet voor internationale uitwisselingen. België heeft die doelstelling gerealiseerd met de wet van 2015.

Het basisprincipe van de CRS is wederkerigheid. De landen ontvangen alleen gegevens indien ze hun eigen gegevens doorgeven. Door de toepassing van wederkerigheid ontstaat een wereldwijd netwerk waarin elk rechtsgebied zowel een bronland (verzender) als een thuisland (ontvanger) is.

Op technisch vlak legt de CRS verplichtingen op aan financiële instellingen. Banken en andere financiële instellingen zijn verplicht de identiteit van buitenlandse

ce qui a fondamentalement levé l'obstacle traditionnel du secret bancaire.

M. Van Quickenborne se penche sur les raisons de la création de la NCD. Dans les années 2000, il est devenu évident que l'échange de données entre États était insuffisant pour lutter contre la fraude fiscale. Le secret bancaire, symbole d'autonomie financière, était perçu comme un obstacle à une perception équitable de l'impôt dans une économie mondialisée. En 2009, le sommet du G20 à Londres, qui s'est tenu immédiatement après la crise financière, a opté pour une nouvelle ère de transparence. L'OCDE a alors été chargée d'élaborer un modèle uniforme permettant la déclaration automatique des données financières. La NCD a été adoptée en juillet 2014, après quatre années de négociations.

Le principal objectif de la NCD est de créer un mécanisme normalisé à l'échelle mondiale pour l'échange automatique d'informations sur les comptes financiers, afin de prévenir l'évasion fiscale transfrontalière. Autrement dit, tandis que le PCC assure le suivi des comptes nationaux, la NCD garantit la détection transnationale. Elle est intégrée à l'Accord multilatéral entre autorités compétentes concernant l'échange automatique de renseignements relatifs aux comptes financiers (*Multilateral Competent Authority Agreement – MCAA*), qui repose sur l'article 6 de la Convention de l'OCDE concernant l'assistance administrative mutuelle en matière fiscale. Ce traité confère aux États le pouvoir d'échanger des informations sur demande, de les partager spontanément ou de le faire automatiquement selon une norme convenue. La Belgique a signé le MCAA en 2014 et s'est engagée à procéder au premier échange automatique en 2017.

La NCD n'est pas directement contraignante, mais son application est rendue possible par la législation nationale. Chaque État participant doit exiger des institutions financières qu'elles collectent des données. Un cadre juridique doit être prévu pour la transmission des données aux autorités fiscales, et un système administratif doit être mis en place pour les échanges internationaux. La Belgique a atteint cet objectif avec la loi de 2015.

Le principe fondamental de la NCD est la réciprocité. Les pays ne reçoivent des données que s'ils transmettent leurs données. L'application de la réciprocité crée un réseau mondial où chaque juridiction constitue à la fois un pays source (émetteur) et un pays de résidence (destinataire).

Sur le plan technique, la NCD impose des obligations aux institutions financières. Les banques et autres établissements financiers sont tenus de déclarer avec

rekeninghouders, het rekeningnummer en het saldo van de rekening op 31 december nauwkeurig aan de nationale belastingdienst te melden. Die verplichte aangifte geldt voor natuurlijke personen, rechtspersonen en hun uiteindelijke begunstigten. Daartoe werd het register van uiteindelijke begunstigten (UBO-register) opgericht.

Financiële instellingen verzamelen de gegevens via een procedure voor klantenidentificatie (KYC). De gegevens worden jaarlijks doorgegeven aan de nationale belastingdienst (in België de Algemene Administratie van de Fiscaliteit van de FOD Financiën), die ze vervolgens doorgeeft aan het woonland van de rekeninghouder via een beveiligd elektronisch kanaal, namelijk het gemeenschappelijk gegevensoverdrachtsysteem van de OESO.

De CRS maakt gebruik van een uniforme gegevensstandaard die zorgt voor wereldwijde interoperabiliteit. Momenteel nemen meer dan 110 rechtsgebieden, oftewel 110 landen, deel aan het CRS-netwerk, waardoor de leemtes worden opgevuld. Het lid vindt dat te weinig.

Wat is de link met de Europese regelgeving? Ten eerste voorzagt de Europese richtlijn uit 2003 betreffende belastingheffing op inkomsten uit spaargelden in de vorm van rentebetaling in een beperkte uitwisseling van informatie over de inkomsten uit rente. Ten gevolge van de financiële crisis bleek die maatregel ontoereikend en werd de richtlijn uit 2011 betreffende de administratieve samenwerking op het gebied van de belastingen (DAC) ingevoerd, die vervolgens werd herzien door de richtlijn uit 2014, DAC2. Die richtlijn verplicht de lidstaten ertoe de CRS ten volle ten uitvoer te leggen, de automatische uitwisseling binnen de EU te organiseren en dezelfde verplichtingen op te leggen aan alle financiële instellingen. De wet uit 2015 behelst de omzetting van de regels uit de CRS en uit DAC2.

Het CAP is weliswaar een nationale databank en de CRS een internationaal netwerk, maar ze vullen elkaar aan: de CAP-wetgeving komt overeen met de identificatie op nationaal niveau (DAC1) en die met betrekking tot de CRS betreft DAC2 (automatische uitwisseling van inlichtingen buiten het nationaal grondgebied). Aldus beschikt België over een uniek en geïntegreerd systeem, bestaande uit een nationaal CAP en een internationale CRS-regeling, die samen instaan voor de opsporing van de rekeningen op nationaal en internationaal niveau.

De CRS berust op drie fundamentele beginselen.

Ten eerste berust de CRS op het finaliteitsbeginsel of principe van doelbinding. Wanneer een buitenlandse rekening aan België wordt gemeld, mag die informatie dus alleen voor fiscale doeleinden worden gebruikt, om te controleren of de rekeninghouder niet heeft verzuimd

exactitude à l'administration fiscale nationale l'identité des titulaires de comptes étrangers, le numéro de compte et le solde du compte au 31 décembre. Cette déclaration concerne les personnes physiques et morales, ainsi que leurs bénéficiaires effectifs. Le registre des bénéficiaires effectifs (UBO) a été créé à cet effet.

Les institutions financières collectent les données via une procédure d'identification du client (KYC). Les données sont transmises annuellement à l'administration fiscale nationale, en l'occurrence l'Administration générale de la Fiscalité du SPF Finances, qui les transmet ensuite au pays de résidence du titulaire du compte via un canal électronique sécurisé: le Système de transfert de données commun (STDC) de l'OCDE.

La NCD utilise une norme de données uniforme garantissant l'interopérabilité mondiale. Actuellement, plus de 110 juridictions, soit 110 pays, participent au réseau NCD, comblant ainsi les lacunes. Le membre est d'avis que ce nombre est trop faible.

Quel est le lien avec la réglementation européenne? Premièrement, la directive européenne de 2003 relative à l'imposition des intérêts d'épargne prévoyait un échange limité d'informations sur les revenus d'intérêts. Suite à la crise financière, cette mesure s'est avérée insuffisante, et la directive de 2011 relative à la coopération administrative en matière fiscale (DAC) a vu le jour, puis a été révisée par la directive de 2014, DAC-2. Cette directive oblige les États membres à mettre pleinement en œuvre la norme NCD, à organiser l'échange automatique au sein de l'UE et à imposer les mêmes obligations à toutes les institutions financières. La loi de 2015 transpose à la fois les règles de la NCD et la directive DAC-2.

Bien que le PCC soit une base de données nationale et la NCD, un réseau international, ils sont complémentaires: la législation relative au PCC correspond à l'identification au niveau national (DAC-1) et celle relative à la NCD concerne la directive DAC-2 (échange automatique hors du territoire national). La Belgique dispose ainsi d'un système unique et intégré, composé d'un PCC national et d'une NCD internationale, qui assurent ensemble la détection des comptes au niveau national et international.

La NCD est fondée sur trois principes fondamentaux.

Premièrement, la NCD repose sur le principe de limitation des finalités. Ainsi, si un compte étranger est communiqué à la Belgique, cette information ne peut être utilisée qu'à des fins fiscales, pour vérifier si le titulaire du compte n'a pas omis de déclarer ce compte

die buitenlandse rekening te vermelden in zijn belastingaangifte. Die informatie gebruiken om gegevens te verkennen, is echter verboden. Een artikel uit de toelichting bij de CRS verduidelijkt dat de gegevens alleen mogen worden gebruikt voor de vaststelling, heffing en aangifte van de belastingen, alsook voor de toepassing van de fiscale wetgeving. Dat betekent dat die gegevens niet mogen worden gekoppeld aan databanken, zoals het CAP, met het oog op profilering of risicoselectie.

Het tweede beginsel betreft de vertrouwelijkheid en veiligheid. Elke deelnemende lidstaat moet strenge veiligheidsnormen garanderen. De OESO voert ook periodieke audits uit om zich ervan te vergewissen dat de lidstaten de beginselen naleven inzake gegevensversleuteling, toegangsbeheer, authenticatie en vernietiging van gegevens na opslag. Lidstaten die deze beginselen niet naleven, kunnen tijdelijk van de uitwisselingscyclus worden uitgesloten.

Ten derde berust de CRS op het wederkerigheidsbeginsel, dat in de eerste plaats ethisch is. Teneinde de strijd tegen belastingontwijking op te voeren, is solidariteit tussen de lidstaten onontbeerlijk. Landen die weigeren informatie te delen, zoals Zwitserland tot 2018, brengen de fiscale rechtvaardigheid in gevaar. Derhalve heeft de CRS een moraliserende functie, door fiscale transparantie vast te stellen als universele norm.

Naast de CRS is er ook nog de FATCA (*Foreign Account Tax Compliance Act*). De FATCA is Amerikaanse regelgeving die in wezen hetzelfde doel nastreeft, maar dan in de betrekkingen tussen de Verenigde Staten en andere landen.

De FATCA berust juridisch op een Amerikaanse wet uit 2010. Die betreft de aangifte van de Amerikaanse belastingplichtigen, terwijl de CRS van de OESO betrekking heeft op de aangifte van niet-ingezetenen uit de hele wereld. Met de FATCA is de wederkerigheid beperkt. De Verenigde Staten ontvangen wel informatie, maar delen die niet, terwijl de CRS berust op wederkerigheid.

Voorts voorziet de FATCA in een bronheffing van 30 % in geval van niet-naleving. De CRS leidt niet tot sancties, maar niet-naleving kan de reputatie van het land schaden. Een land dat weinig meewerkt, geen wederkerigheid toepast of de CRS ondoeltreffend ten uitvoer legt, kan publiekelijk aan de kaak worden gesteld.

De Europese implementatie van de FATCA gebeurde via zogenoemde intergouvernementele overeenkomsten (IGA). De CRS werd dan weer ten uitvoer gelegd via DAC2. België heeft de twee systemen, de FATCA en de

étranger dans sa déclaration d'impôts. Mais l'utilisation de ces données à des fins d'exploration de données est interdite. Un article du Commentaire de la NCD précise que les données ne peuvent être utilisées que pour l'établissement, le prélèvement et la déclaration des impôts, ainsi que pour l'application de la législation fiscale. Cela signifie que ces données ne peuvent être reliées à des bases de données, telles que le PCC, à des fins de profilage ou de sélection des risques.

Le deuxième principe est celui de confidentialité et de sécurité. Chaque État membre participant doit garantir des normes de sécurité strictes. L'OCDE réalise également des audits périodiques pour s'assurer que les États membres respectent les principes de chiffrement des données, de gestion des accès, d'authentification et de destruction des données après leur conservation. Si les États ne respectent pas ces principes, ils peuvent être temporairement exclus du cycle d'échange.

Troisièmement, la NCD est basée sur le principe de réciprocité, qui est avant tout éthique. Pour intensifier la lutte contre l'évasion fiscale, la solidarité entre les États membres est indispensable. Les pays qui refusent de partager des informations, comme la Suisse jusqu'en 2018, compromettent l'équité fiscale. Par conséquent, la NCD a une fonction moralisatrice, en établissant la transparence fiscale comme norme universelle.

À la NCD s'ajoute le règlement FATCA (*Foreign Account Tax Compliance Act*). Le FATCA est un règlement américain unilatéral qui poursuit essentiellement le même objectif, mais dans les relations entre les États-Unis et les pays étrangers.

Le FATCA est fondé juridiquement sur une loi américaine unilatérale de 2010. Il concerne la déclaration des contribuables américains, tandis que la NCD de l'OCDE concerne la déclaration des non-résidents du monde entier. Avec le règlement FATCA, la réciprocité est limitée. Les États-Unis reçoivent les informations mais ne les partagent pas, alors que la norme NCD repose sur la réciprocité.

Par ailleurs, le FATCA prévoit une retenue à la source de 30 % en cas de non-conformité. La norme NCD n'entraîne aucune sanction, mais ne pas l'observer peut nuire à la réputation du pays. Un pays qui participe peu, ne pratique pas la réciprocité ou met en œuvre la norme NCD de manière inefficace peut être publiquement dénoncé.

La mise en œuvre européenne du FATCA s'est faite par le biais d'accords intergouvernementaux (IGAs). La norme NCD, quant à elle, a été mise en œuvre par la directive DAC-2. La Belgique a intégré les deux systèmes,

CRS, in één wet opgenomen. Het resultaat is een internationaal netwerk met twee niveaus: het FATCA-netwerk voor informatie bestemd voor de Verenigde Staten en het CRS-netwerk voor informatie bestemd voor meer dan 100 andere landen.

Vervolgens gaat de heer Van Quickenborne dieper in op de mondiale reikwijdte van de CRS. Volgens OESO-cijfers uit 2023 hebben meer dan 110 rechtsgebieden samen meer dan 123 miljoen rekeningen, goed voor een totale waarde van meer dan 12.000 miljard Amerikaanse dollar. De automatische uitwisseling heeft geleid tot een toename van vrijwillige regularisaties en een daling van het aantal offshorerekeningen.

België ontvangt jaarlijks uit meer dan 70 partnerlanden gegevens over 10.000 buitenlandse rekeningen van zijn inwoners. In ruil daarvoor rapporteert België gegevens over niet-inwoners aan de respectieve bevoegde belastingautoriteiten.

De CRS heeft de fiscale opsporing van buitenlandse inkomsten ingrijpend veranderd, wat de transparantie aanzienlijk ten goede is gekomen. Terwijl het CAP de mogelijkheid biedt Belgische rekeningen te identificeren, laat de CRS ook toe de Luxemburgse, Zwitserse of Singaporese rekeningen van Belgische inwoners te traceren.

Wat hun respectieve rechtsposities betreft, zijn het CAP en de CRS complementair, maar ze overlappen elkaar niet en hebben verschillende reikwijdtes en functies. Het CAP laat nationale identificatie van de binnenlandse rekeningen toe. De CRS zorgt voor de internationale rapportage van buitenlandse rekeningen. Hun relatie is horizontaal en ze vullen elkaar aan in de keten van fiscale transparantie. Het CAP maakt interne controle mogelijk, de CRS externe detectie.

Wat is het verschil in rechtsgrondslag tussen het CAP en de CRS? Het CAP komt voort uit de wet van 14 april 2011, de CRS uit die van 16 december 2015. Het CAP is een nationaal administratief register, de CRS een internationaal uitwisselingsmechanisme. Het CAP wordt beheerd door de Nationale Bank van België, de CRS door de FOD Financiën. De CAP-gegevens omvatten IBAN-nummers, namen, openings- en sluitingsdatums, financiële gegevens en saldi. Bij de CRS zijn dat onder meer de saldi. Volgens de spreker worden de dividenden en interesten ook via de CRS gerapporteerd, maar dat zal de minister kunnen bevestigen.

Tot het CAP hebben alleen binnenlandse overheden toegang. De CRS is dan weer alleen toegankelijk voor buitenlandse belastingdiensten. Het CAP heeft tot nu toe gediend voor onderzoek en invordering, maar volgens

FATCA en NCD, dans une loi unique. Il en résulte un réseau international à deux niveaux: le réseau FATCA pour les informations destinées aux États-Unis et le réseau NCD pour les informations destinées à plus de 100 autres pays.

M. Van Quickenborne se penche sur la portée mondiale de la NCD. Selon les chiffres de l'OCDE de 2023, plus de 110 juridictions détiennent conjointement plus de 123 millions de comptes et déclarent une valeur totale de plus de 12.000 milliards de dollars américains. L'échange automatique a entraîné une augmentation des régularisations volontaires et une diminution du nombre de comptes offshore.

La Belgique reçoit chaque année les données de 10.000 comptes étrangers de ses résidents, provenant de plus de 70 pays partenaires. En retour, la Belgique communique des données sur les non-résidents aux autorités fiscales compétentes.

La NCD a radicalement transformé le suivi fiscal des revenus étrangers, améliorant considérablement la transparence. Le PCC permet d'identifier les comptes belges et la NCD permet de suivre les comptes luxembourgeois, suisses ou singapouriens des résidents belges.

Pour ce qui est de leur position juridique respective, le PCC et la NCD sont des systèmes complémentaires, mais qui ne se chevauchent pas et ont des portées et des fonctions différentes. Le PCC permet l'identification nationale des comptes nationaux. La NCD permet la déclaration internationale des comptes étrangers. La relation est horizontale et ils se complètent dans la chaîne de la transparence fiscale. Le PCC permet le contrôle interne, tandis que la NCD permet la détection externe.

Quelle est la différence de base juridique entre le PCC et la NCD? Le PCC émane de la loi du 14 avril 2011, la NCD de celle du 16 décembre 2015. Le PCC est un registre administratif national et la NCD est un mécanisme d'échange international. La Banque nationale de Belgique administre le PCC, et le SPF Finances administre la NCD. Les données du PCC sont: l'IBAN, les noms, les dates d'ouverture et de fermeture, les coordonnées financières et les soldes. La NCD inclut les soldes. Le membre pense que les dividendes et les intérêts sont également déclarés via la NCD, mais il demande confirmation au ministre.

Seules les autorités nationales ont accès au PCC. Concernant la NCD, seules les autorités fiscales étrangères y ont accès. Le PCC a pour objectif actuel l'enquête et le recouvrement, mais M. Van Quickenborne pense qu'à

de heer Van Quickenborne zal het op termijn uitgroeien tot een instrument voor *money control*. De CRS is dan weer bedoeld voor automatische fiscale samenwerking. Beide systemen vallen onder artikel 22 van de Belgische Grondwet en artikel 22 van de algemene verordening gegevensbescherming (AVG). Hun werking verschilt echter. Het CAP is reactief en kan alleen op verzoek worden geraadpleegd, terwijl de CRS proactief werkt.

Het lid concludeert daaruit dat de CRS de internationale afspiegeling tot stand brengt van het Belgische CAP. Beide beogen dezelfde doelstelling, met name fiscale transparantie, maar vanuit twee verschillende perspectieven. De CRS kijkt van buitenaf naar binnen door buitenlandse rekeningen van inwoners te screenen. Het CAP kijkt van binnen naar buiten door de Belgische rekeningen van inwoners te onderzoeken. Zo vormen ze een tweeluik van moderne fiscale openheid, waarin privacy en doeltreffendheid voortdurend tegen elkaar moeten worden afgewogen.

De CRS is in Belgisch recht omgezet met de wet van 16 december 2015. Die wet is bijzonder omdat hij een dubbel doel dient, met name zowel de Europese DAC2-richtlijn uit 2014 (2014/107/EU) als de CRS van de OESO omzetten in nationaal recht. De wet verplicht financiële instellingen om jaarlijks gegevens over niet-ingezeten rekeninghouders te rapporteren aan de FOD Financiën en om die informatie uit te wisselen met de belastingautoriteiten van de woonstaat van die rekeninghouders. Dat is een wederkerig mechanisme. België ontvangt ook gegevens van Belgische inwoners die rekeningen aanhouden in deelnemende landen.

De bewuste wet bestaat uit drie hoofdonderdelen. Ten eerste de definities en het toepassingsgebied. In hoofdstuk 1 wordt bepaald wat men verstaat onder financiële instellingen, rekeninghouder en rapportage, in lijn met de bijlagen omtrent de OESO-CRS. Hoofdstuk 2 gaat over de rapportageverplichtingen. Hoofdstuk 3 betreft de gegevensuitwisseling en de vertrouwelijkheid, en beschrijft de voorwaarden waaronder de overheid via het CTS van de OESO gegevens doorstuurt naar andere landen.

Een koninklijk besluit regelt de technische nadere regels inzake het rapportageformaat, de beveiligingsnormen en de bewaartermijnen. De FOD Financiën heeft binnen de Algemene Administratie van de Fiscaliteit een CRS-DAC2-contactpunt opgericht dat de operationele coördinatie verzorgt.

De heer Van Quickenborne licht uitvoerig de wettelijke verplichtingen toe die rusten op financiële instellingen in het kader van de Belgische implementatie van de

terme, il s'agira d'un outil de *money control*. La NCD, quant à elle, vise la coopération fiscale automatique. Les deux dispositifs sont soumis à l'article 22 de la Constitution belge, ainsi qu'à l'article 22 du Règlement général sur la protection des données (RGPD). Cependant, leur fonctionnement diffère. Le PCC est réactif et ne peut être consulté que sur demande, tandis que la NCD est proactive.

Le membre en conclut que la NCD est le pendant international du PCC belge. L'une et l'autre poursuivent le même objectif, à savoir la transparence fiscale, mais selon deux perspectives différentes. La NCD examine les comptes étrangers des résidents de l'extérieur vers l'intérieur. Le PCC, quant à lui, examine les comptes belges des résidents de l'intérieur vers l'extérieur. Ils forment ainsi un diptyque de la transparence fiscale moderne, où confidentialité et efficacité doivent être constamment conciliées.

La NCD a été transposée en droit belge à travers la loi du 16 décembre 2015. Cette loi est particulière car elle poursuit un double objectif: transposer en droit national, à la fois, la directive européenne DAC-2 de 2014 (2014/107/UE) et la NCD de l'OCDE. Cette loi oblige les institutions financières à déclarer annuellement au SPF Finances les données relatives aux titulaires de comptes non-résidents et à échanger ces informations avec les autorités fiscales du pays de résidence de ces titulaires. Ce mécanisme est réciproque. La Belgique reçoit également des données de ses résidents détenant des comptes dans les pays participants.

La loi en question se compose de trois parties principales. Premièrement, les définitions et le champ d'application. Le chapitre 1 définit les notions d'institutions financières, de titulaires de comptes et de déclaration, conformément aux annexes de la NCD de l'OCDE. Le chapitre 2 porte sur les obligations de déclaration. Le chapitre 3 concerne l'échange de données et la confidentialité et définit les conditions dans lesquelles l'administration transmet des données à d'autres États via le STDC de l'OCDE.

Un arrêté royal a été publié, qui fixe les modalités techniques relatives au format de la déclaration, aux normes de sécurité et aux durées de conservation. Le SPF Finances a mis en place un point de contact, NCD DAC-2, au sein de l'Administration générale de la Fiscalité du SPF Finances, qui assure la coordination opérationnelle.

M. Van Quickenborne détaille les obligations légales qui incombent aux institutions financières dans le cadre de la transposition en droit belge (loi du 16 décembre

Common Reporting Standard (CRS), zoals ingevoerd bij de wet van 16 april 2015. Hij schetst een driedelige structuur: identificatie, rapportering en sancties.

Hij preciseert dat financiële instellingen bij de identificatie van rekeninghouders verplicht zijn een “*self-certification*” procedure toe te passen. Nieuwe klanten moeten bij het openen van een rekening hun fiscale woonstaat en hun TIN (*Tax Identification Number*) meedelen. Voor reeds bestaande klanten gebeurt een zogenaamde “*look-back review*”, gebaseerd op de reeds beschikbare klantgegevens.

Wat de rapportering betreft, legt hij uit dat per rekeninghouder onder meer naam, adres, geboortedatum, TIN, rekeningnummer, het saldo op 31 december en bepaalde inkomsten (zoals intresten, dividenden en opbrengsten uit financiële activa) moeten worden doorgestuurd. Deze gegevens worden in XML-formaat, volgens het OESO-schema, elektronisch aangeleverd.

Bij niet-naleving kunnen administratieve geldboetes tot 50.000 euro worden opgelegd. In ernstige gevallen kan strafrechtelijke vervolging volgen wegens belemmering van de fiscale controle. België riskeert bovendien internationale sancties, waaronder de opschorting van gegevensuitwisseling bij structurele tekortkomingen.

Vervolgens gaat de spreker in op het beheer van de CRS-gegevens in België. De FOD Financiën, zo benadrukt hij, is de verwerkingsverantwoordelijke in de zin van de GDPR en beheert de gegevens in een strikt gescheiden CRS-databank, onafhankelijk van het Centraal Aanspreekpunt (CAP). Die scheiding moet vermenging van gegevens tegengaan. De wet voorziet in een bewaartermijn van vijf jaar voor CRS-gegevens, terwijl voor het CAP een termijn van tien jaar geldt op basis van het *Multilateral Competent Authority Agreement* (MCAA). De administratie moet daarnaast instaan voor logging, interne toegangscontroles en de versleuteling van de gegevens.

De heer Van Quickenborne herinnert eraan dat CRS-gegevens onder de huidige wetgeving uitsluitend voor fiscale doeleinden mogen worden gebruikt en dat het aanwenden ervan voor risicoanalyse of datamining verboden blijft, tenzij een wet daarin voorziet. Net dat is volgens hem wat het voorliggend amendement beoogt: het toelaatbaar maken van datamining binnen het data-warehouse van de FOD Financiën, door CAP-gegevens – inclusief informatie over buitenlandse rekeningen – in dat systeem op te nemen.

2015) de la norme commune de déclaration (*Common Reporting Standard* ou CRS). Il décrit une structure en trois couches, à savoir l'identification, la déclaration et les sanctions.

Il précise que les institutions financières sont tenues d'appliquer une procédure d'auto-certification lors de l'identification des titulaires de comptes. Les nouveaux clients doivent communiquer leur pays de résidence fiscale et leur numéro d'identification fiscale (*Tax Identification Number*) lors de l'ouverture d'un compte. Pour les clients existants, un examen rétrospectif est réalisé sur la base de leurs données déjà disponibles.

En ce qui concerne la déclaration proprement dite, le membre explique que, pour chaque titulaire de compte, il faut notamment transmettre son nom, son adresse, sa date de naissance, son numéro d'identification fiscale, son numéro de compte, le solde au 31 décembre et certains de ses revenus (notamment les intérêts, les dividendes et les revenus provenant d'actifs financiers). Ces données sont transmises par voie électronique au format XML, conformément au schéma de l'OCDE.

En cas de non-respect, des amendes administratives pouvant aller jusqu'à 50.000 euros peuvent être infligées. Dans les cas graves, des poursuites pénales peuvent être engagées pour obstruction au contrôle fiscal. La Belgique risque en outre des sanctions internationales, notamment la suspension de l'échange de données en cas de manquements structurels.

L'intervenant aborde ensuite la gestion des données CRS en Belgique. Il souligne que le SPF Finances est le responsable du traitement au sens du RGPD et qu'il gère les données dans une banque de données CRS strictement séparée et indépendante du Point de contact central (PCC). Cette séparation vise à empêcher tout croisement des données. La loi prévoit une durée de conservation de cinq ans pour les données CRS, contre dix ans pour le PCC sur la base du modèle multilatéral d'accord entre autorités compétentes. L'administration doit en outre assurer la journalisation, les contrôles d'accès internes et le chiffrement des données.

M. Van Quickenborne rappelle que, dans sa formulation actuelle, la législation dispose que les données CRS ne peuvent être utilisées qu'à des fins fiscales et que leur utilisation à des fins d'analyse de risque ou de *data mining* reste interdite, sauf si une loi l'autorise. Or, l'amendement à l'examen tend précisément à permettre le *data mining* dans le *data warehouse* du SPF Finances, en intégrant les données du PCC – y compris les informations relatives aux comptes étrangers – dans ce système.

Daarna bespreekt hij de verhouding tussen CRS en CAP. Hoewel beide systemen op het eerste gezicht gelijkaardige informatie bevatten, zijn hun doelstelling, toegang, modaliteiten en juridische basis volgens hem fundamenteel verschillend. Het CAP, op nationaal niveau, wordt beheerd door de Nationale Bank; de CRS-databank, op internationaal niveau, door de FOD Financiën. De wetgever heeft bewust gekozen voor een institutionele scheiding van beide infrastructuren, om zo de indruk van één allesomvattend register te vermijden en de doelbinding van elke verwerking te garanderen.

Het commissielid beschrijft vervolgens hoe de informatieketen in de praktijk werkt. Wanneer de fiscus een discrepantie vaststelt tussen de aangegeven inkomsten van een belastingplichtige en diens levensstijl – de zogenaamde indiciaire tekorten op basis van artikel 322, § 3 WIB 92 – kan de administratie het CAP raadplegen om te achterhalen bij welke Belgische banken de betrokkene rekeningen heeft. Indien aan de voorwaarden voor het opheffen van het bankgeheim is voldaan, kan vervolgens ook worden onderzocht of CRS-gegevens aangeven dat die persoon buitenlandse rekeningen bezit. Op die manier vormen CAP en CRS niet één samengevoegde databron, maar twee opeenvolgende schakels binnen eenzelfde procedurele keten. De spreker illustreert dit met een voorbeeld waarbij de levensstijl – zoals het rijden met een zeer exclusieve wagen – niet strookt met het aangegeven inkomen.

Tot slot gaat hij in op de constitutionele en privacy-rechtelijke beoordeling van deze systemen. Hij stelt dat zowel het CAP als de CRS-regeling bij wet zijn ingevoerd, waardoor het legaliteitsbeginsel van artikel 22 van de Grondwet en artikel 8 EVRM is gerespecteerd. Verder zijn de AVG-beginselen van transparantie, minimalisatie en beveiliging volledig geïntegreerd in de verwerking van gegevens. Volgens hem is de bestaande rechtsgrond voor CAP-verwerkingen dus solide. Hij verduidelijkt daarbij dat hij het niet heeft over het systeem dat via amendement zou worden ingevoerd en de verruiming van datamining beoogt, door critici ironisch “*money control*” genoemd.

Hij verwijst vervolgens uitvoerig naar het zogeheten Valentijnsarrest van het Grondwettelijk Hof van 14 februari 2013, dat een driedelig proportionaliteitscriterium hanteert: de inmenging moet strikt noodzakelijk zijn, een wettig doel nastreven en omkaderd zijn door effectieve waarborgen tegen misbruik. Verschillende deskundigen, zo geeft hij aan, beschouwen dit arrest als een mogelijke voorbode van een toekomstig verzoek tot vernietiging van de nieuwe wet indien deze zou worden aangenomen. In

Le membre poursuit en évoquant la relation entre le CRS et le PCC. Bien que les deux systèmes contiennent à première vue des informations similaires, leur finalité, leur accès, leurs modalités et leur base juridique sont, selon lui, fondamentalement différents. Le PCC est géré, au niveau national, par la Banque nationale, tandis que le SPF Finances assure la gestion de la banque de données CRS au niveau international. Le législateur a délibérément cloisonné ces deux infrastructures sur le plan institutionnel, afin de ne pas donner l'impression d'un registre global et de respecter la limitation des finalités de chaque traitement.

Le membre décrit ensuite comment fonctionne la chaîne d'information en pratique. Lorsque l'administration fiscale constate une anomalie entre les revenus déclarés d'un contribuable et son train de vie – ce que l'on appelle les déficits indiciaires sur la base de l'article 322, § 3, du CIR 92 –, elle peut consulter le PCC pour identifier les banques belges auprès desquelles la personne concernée possède des comptes. Si les conditions de levée du secret bancaire sont remplies, elle peut ensuite consulter les données CRS pour vérifier si cette personne possède des comptes à l'étranger. Le PCC et le CRS ne constituent ainsi pas une source de données unique, mais deux maillons successifs au sein d'une même chaîne procédurale. L'intervenant donne l'exemple d'une personne qui roule en voiture de luxe pour illustrer la discordance qui peut exister entre son style de vie et son revenu déclaré.

Enfin, il aborde le contrôle de constitutionnalité et de légalité de ces systèmes sous l'angle de la vie privée. Il indique que tant le PCC que le CRS ont été instaurés par la loi, ce qui respecte le principe de légalité visé à l'article 22 de la Constitution et à l'article 8 de la CEDH. En outre, les principes de transparence, de minimisation et de sécurité prévus par le RGPD sont pleinement intégrés dans le traitement des données. Selon M. Van Quickenborne, les traitements effectués dans le cadre du PCC reposent donc actuellement sur une base juridique solide. Il précise qu'il n'entend pas par là le système que l'amendement à l'examen tend à instaurer et qui vise à étendre l'utilisation du PCC au *data mining*, que ses détracteurs qualifient ironiquement de “*money control*”.

L'intervenant commente ensuite en détail “l'arrêt de la Saint-Valentin” rendu par la Cour constitutionnelle le 14 février 2013. La Cour y subordonne le critère de proportionnalité à trois éléments: l'ingérence doit être strictement nécessaire, poursuivre un objectif légitime et être encadrée par des garanties effectives contre les abus. Le membre indique que plusieurs experts considèrent cet arrêt comme le présage éventuel d'un futur recours en annulation de la nouvelle loi si celle-ci

dat licht acht hij het uiterst relevant om de verenigbaarheid van het amendement met dit proportionaliteitskader te onderzoeken.

De heer Van Quickenborne besluit dat de toepassing van het Valentijnsarrest op de voorliggende wetgeving een bijzonder interessante juridische oefening zal vormen, mocht deze wetgeving daadwerkelijk worden aangenomen.

De heer Van Quickenborne vervolgt zijn uiteenzetting met de vaststelling dat zowel het CAP-systeem als de CRS-wetgeving de proportionaliteitstoets van het Valentijnsarrest met succes hebben doorstaan. Volgens hem is dat te danken aan drie elementen: het duidelijk omschreven doel van internationale fiscale samenwerking, de beperking tot strikt relevante gegevens, en het bestaan van effectieve externe controle door de GBA en de periodieke audits van de OESO.

De spreker en wijst erop dat het gebruik van CRS-gegevens voor algoritmische analyse of risicoprofilering – dus voor datamining – onder de huidige regelgeving verboden is. De wet van 16 december 2015, die de automatische internationale uitwisseling van inlichtingen regelt, staat dergelijke verwerking niet toe. Een dergelijke stap zou een nieuwe formele wettelijke basis vereisen, die bovendien opnieuw een grondwettelijke toetsing zou moeten doorstaan. Hij benadrukt dat het Valentijnsarrest een duidelijke grens trekt: algemene screening zonder individuele aanleiding is onverenigbaar met het recht op privacy.

De heer Van Quickenborne wijst erop dat er een dubbele controle bestaat op de naleving van gegevensbeschermingsnormen binnen de FOD Financiën: nationaal door de GBA, en internationaal door de OESO via vertrouwelijkheidsaudits. Samen moeten zij verzekeren dat België voldoet aan strenge normen inzake dataprotectie.

Daarna bespreekt hij de effectiviteit van de CRS. België heeft volgens hem sinds de invoering een duidelijke stijging vastgesteld in vrijwillige regularisaties van buitenlandse activa. De CRS zorgt bovendien voor betere zichtbaarheid van buitenlandse tegoeden en versterkt de samenwerking met buurlanden zoals Nederland en Luxemburg. Ook de combinatie van CAP en CRS leidt tot meer coherente fiscale dossiers en snellere fraudeopsporing.

Hij plaatst daartegenover evenwel enkele structurele beperkingen. Zo varieert de datakwaliteit sterk van land tot

venait à être adoptée. Dans cette optique, il estime qu'il est tout à fait pertinent d'examiner la compatibilité de l'amendement à l'examen au regard de ce cadre de proportionnalité.

M. Van Quickenborne conclut ce point en indiquant qu'il sera particulièrement intéressant d'appliquer les conclusions de l'arrêt précité à la législation en projet si celle-ci vient effectivement à être adoptée.

Le membre poursuit son exposé en constatant que tant le système du PCC que la législation relative au CRS ont passé avec succès le test de proportionnalité de l'arrêt de la Saint-Valentin. Il pointe trois éléments pour expliquer ces résultats: la finalité clairement définie de la coopération fiscale internationale, la limitation aux données strictement pertinentes et, enfin, l'existence d'un contrôle externe efficace réalisé par l'APD et d'audits périodiques de l'OCDE.

L'intervenant souligne que l'utilisation des données CRS à des fins d'analyse algorithmique ou de profilage des risques – c'est-à-dire à des fins de data mining – est interdite par la réglementation actuelle. La loi du 16 décembre 2015, qui encadre l'échange automatique de renseignements au niveau international, n'autorise en effet pas ce type de traitement. Une telle mesure nécessiterait une nouvelle base légale formelle, qui devrait en outre résister à l'épreuve d'un nouveau contrôle de constitutionnalité. Le membre souligne que l'arrêt de la Saint-Valentin trace une limite claire: le screening général sans motif individuel est incompatible avec le droit à la vie privée.

M. Van Quickenborne indique qu'il existe un double contrôle du respect des normes en matière de protection des données au sein du SPF Finances: l'un est réalisé au niveau national par l'APD et l'autre, au niveau international par l'OCDE dans le cadre des audits de confidentialité des données. Ensemble, ces deux organisations doivent veiller à ce que la Belgique respecte les normes strictes en matière de protection des données.

Il évoque ensuite l'efficacité du CRS. Selon lui, la Belgique a constaté, depuis l'introduction de cette norme, une nette augmentation des régularisations volontaires d'actifs étrangers. Le CRS assure en outre une meilleure visibilité des avoirs étrangers et renforce la coopération avec les pays voisins tels que les Pays-Bas et le Luxembourg. La combinaison du PCC et du CRS permet également de renforcer la cohérence des dossiers fiscaux et d'accélérer la détection des fraudes.

Il épingle toutefois plusieurs obstacles structurels. Par exemple, la qualité des données varie considérablement

land, leveren automatische uitwisselingen soms enorme hoeveelheden gegevens op die moeilijk te interpreteren zijn, en blijft de juridische ruimte voor koppeling met andere databanken beperkt. De grootste uitdaging voor de toekomst is volgens hem dan ook niet de kwantiteit van de data, maar de kwaliteit van de analyse. Hij verwijst naar gesprekken met dataminers en leidinggevendenden binnen de fiscale administratie, die aangeven dat men vandaag eerder “verdrinkt in de data” dan dat men data te kort komt. Het vooruitzicht dat er via het amendement honderden miljoenen nieuwe datapunten zouden worden toegevoegd, baart hem ernstige zorgen voor de werkbaarheid en efficiëntie.

Aansluitend formuleert de spreker enkele beleidsaanbevelingen. Hij pleit vooreerst voor het behoud van het duale systeem CAP-CRS, dat volgens hem in binnen- en buitenland wordt erkend als evenwichtig en privacybestendig. Indien de regering – zoals in de verantwoording van het amendement wordt gesuggereerd – zou overwegen om beide systemen te integreren in één databank, dan moet volgens hem eerst een volledig wetgevingsproces worden doorlopen. In dat geval zou immers niet alleen het CAP-kader moeten worden aangepast, maar ook de CRS-wet van 16 december 2015, waarnaar in de huidige toelichting geen enkele verwijzing te vinden is. Hij noemt dit een manifest gebrek in de motivering van het amendement.

Daarnaast dringt hij aan op een structurele parlementaire controle. De Kamer zou volgens hem jaarlijks een gedetailleerd verslag moeten ontvangen over het aantal CRS-gegevensuitwisselingen, de doeltreffendheid van beide systemen en de naleving van privacyregels. Hij wijst erop dat de Nederlandse Tweede Kamer op dat vlak een *best practice* vormt, terwijl de Belgische parlementaire informatievoorziening over CAP en CRS beperkt blijft tot antwoorden van de minister op occasionele schriftelijke vragen.

Verder pleit de heer Van Quickenborne voor versterkte internationale samenwerking, met name binnen de OESO en de Europese Unie, om de kwaliteit van CRS-gegevens te verbeteren en systematischer feedback te ontvangen over fouten of inconsistenties. Hij vraagt de minister uitdrukkelijk of de CRS inmiddels ook geldt voor cryptomunten en digitale platformen, aangezien hierover op dit moment weinig duidelijkheid bestaat.

De spreker bundelt vervolgens zijn voorgaande opmerkingen in een bredere conclusie. Volgens hem markeert de CRS-wet van 2015 de overgang van het tijdperk van nationaal bankgeheim naar een regime van

d'un pays à l'autre, les échanges automatiques fournissent parfois d'énormes quantités de données difficiles à interpréter et la marge de manœuvre juridique permettant d'établir des connexions avec d'autres banques de données reste limitée. Selon l'intervenant, le défi majeur pour l'avenir ne réside donc pas dans la quantité de données, mais bien dans la qualité de leur analyse. Il renvoie à des discussions avec des spécialistes de l'exploration des données et des responsables de l'administration fiscale, qui indiquent qu'aujourd'hui, ils “croulent sous les données” plutôt que d'en manquer. La perspective que l'amendement visé introduise des centaines de millions de nouveaux points de données le préoccupe sérieusement en termes de faisabilité et d'efficacité.

Dans la foulée, l'intervenant formule plusieurs recommandations politiques. Il préconise d'abord de maintenir le système dual PCC-CRS, qui, selon lui, est reconnu tant au niveau national qu'international comme étant équilibré et respectueux de la vie privée. Si le gouvernement envisageait, comme le suggère la justification de l'amendement, d'intégrer les deux systèmes dans une seule banque de données, il estime qu'il faudrait d'abord mener un processus législatif complet. Dans ce cas, il faudrait en effet modifier non seulement le cadre PCC, mais également la loi CRS du 16 décembre 2015, à laquelle la justification actuelle ne renvoie aucunement. Il estime qu'il s'agit d'une lacune manifeste dans la justification de l'amendement.

Il demande aussi un contrôle parlementaire structurel. Selon lui, la Chambre devrait recevoir chaque année un rapport détaillé sur le nombre d'échanges de données CRS, sur l'efficacité des deux systèmes et sur le respect des règles en matière de protection de la vie privée. Il souligne que la chambre basse du Parlement néerlandais constitue un exemple à suivre dans ce domaine, alors que les informations transmises aux parlementaires belges à propos du PCC et du CRS se limitent aux réponses apportées par le ministre à des questions écrites occasionnelles.

M. Van Quickenborne préconise également un renforcement de la coopération internationale, notamment au sein de l'OCDE et de l'Union européenne, afin d'améliorer la qualité des données provenant du CRS et d'obtenir un feedback plus systématique sur les erreurs ou les incohérences. Il demande expressément au ministre si le CRS s'applique désormais également aux cryptomonnaies et aux plateformes numériques, compte tenu du manque de clarté existant aujourd'hui à ce sujet.

L'intervenant regroupe ensuite ses observations précédentes dans une conclusion plus large. Selon lui, la loi CRS de 2015 marque la transition de l'ère du secret bancaire national vers un régime de transparence fiscale

gecontroleerde mondiale fiscale transparantie. CAP en CRS vormen daarbij twee complementaire bouwstenen: het ene op nationaal niveau, het andere op internationaal niveau. Beide zijn strikt wettelijk verankerd, proportioneel begrensd en onderworpen aan onafhankelijke controlemechanismen. De grondwettelijke legitimiteit van dit geheel rust volgens hem op drie pijlers: een nauwkeurige wettelijke basis, een duidelijke afbakening van doel en bevoegdheid, en effectieve waarborgen en toezicht.

Zolang die voorwaarden worden geëerbiedigd, blijft België binnen de grenzen van artikel 32 van de Grondwet en artikel 8 EVRM. Zodra men echter – zoals via data-mining – gegevens buiten de strikt toegestane doeleinden zou beginnen te verwerken, komt volgens hem de legitimiteit van het volledige systeem in gevaar.

Hij besluit met de vaststelling dat het Belgische transparantiemodel, opgebouwd rond de CAP-wet van 8 juli 2018 en de CRS-wet van 2015, momenteel een van de meest coherente Europese systemen vormt. Het waarborgt dat de fiscus over de nodige informatie beschikt zonder het vertrouwen van burgers in de rechtsstaat te ondermijnen. De echte uitdaging voor de toekomst ligt volgens hem in het beschermen van dit evenwicht binnen een digitale omgeving waarin de verleiding groot is om datavolume en efficiëntie boven rechtsstatelijkheid te plaatsen. Hij stelt dat het amendement “*money control*” precies in die verleiding dreigt te vervallen.

Na het luik over de *Common Reporting Standard* wenst het commissielid stil te staan bij de impact van de Amerikaanse *Foreign Account Tax Compliance Act* (FATCA) op de Belgische fiscale wetgeving. Hij zal ingaan op het juridisch kader van FATCA, de Belgische implementatie ervan via een bilaterale *Intergovernmental Agreement* (IGA), de relatie met het CAP-systeem en de beleidsmatige en grondwettelijke implicaties van deze internationale gegevensuitwisseling.

De heer Van Quickenborne schetst eerst de ontstaanscontext van de FATCA-wetgeving. Het Amerikaanse Congres neemt in maart 2010 de *Foreign Account Tax Compliance Act* aan, nadat zowel het Huis van Afgevaardigden als de Senaat de tekst hebben goedgekeurd. Het doel van die wet is om belastingontduiking door Amerikaanse belastingplichtigen via buitenlandse rekeningen tegen te gaan.

FATCA verplicht alle buitenlandse financiële instellingen – de zogeheten *Foreign Financial Institutions* (FFI's) – om Amerikaanse rekeninghouders te identificeren en hun financiële gegevens jaarlijks door te sturen aan de Internal Revenue Service (IRS). Een eenvoudig voorbeeld

mondiale controle. Le PCC et le CRS constituent à cet égard deux piliers complémentaires: l'un au niveau national, l'autre au niveau international. Ils sont tous deux strictement inscrits dans la loi, limités de manière proportionnée et soumis à des mécanismes de contrôle indépendants. Selon lui, la légitimité constitutionnelle de cet ensemble repose sur trois piliers: une base juridique précise, une délimitation claire de la finalité et de la compétence, ainsi que des garanties et un contrôle effectifs.

Tant que ces conditions seront respectées, la Belgique respectera les limites fixées par l'article 32 de la Constitution et l'article 8 de la ConvEDH. Mais dès que des données commenceront à être traitées à des fins autres que celles strictement autorisées, comme dans le cadre de l'exploration des données, la légitimité de l'ensemble du système sera, selon lui, compromise.

Il conclut en constatant que le modèle belge de transparence, bâti sur la loi PCC du 8 juillet 2018 et de la loi CRS de 2015, est actuellement l'un des systèmes européens les plus cohérents. En effet, ce système garantit que l'administration fiscale dispose des informations nécessaires sans saper la confiance des citoyens dans l'état de droit. Selon l'intervenant, le véritable défi à l'avenir sera de préserver cet équilibre dans un environnement numérique où la tentation sera grande de privilégier le volume de données et l'efficacité au respect de l'état de droit. Or, il estime qu'au travers de l'amendement *money control*, on risque justement de succomber à cette tentation.

Après le volet consacré au *Common Reporting Standard*, l'intervenant souhaite s'attarder sur l'incidence de la loi américaine *Foreign Account Tax Compliance Act* (FATCA) sur la législation fiscale belge. Il évoquera le cadre juridique de la FATCA, sa mise en œuvre par la Belgique dans le cadre d'un accord intergouvernemental bilatéral (AIG), sa relation avec le système du PCC et les implications politiques et constitutionnelles de cet échange international de données.

M. Van Quickenborne commence par décrire la genèse de la législation FATCA. En mars 2010, le Congrès américain a adopté la *Foreign Account Tax Compliance Act*, après l'adoption du texte par la Chambre des représentants et le Sénat. Cette loi vise à lutter contre la fraude fiscale commise par des contribuables américains à l'aide de comptes étrangers.

La FATCA oblige tous les établissements financiers étrangers – les *Foreign Financial Institutions* (FFI) – à identifier les titulaires de comptes américains et à transmettre chaque année leurs données financières à l'Internal Revenue Service (IRS). Un exemple simple illustre ce

illustreert dit: wanneer de nieuwe Amerikaanse ambassadeur in België een rekening opent, moet de bank vaststellen dat hij een “*US person*” is en vervolgens diens rekeninggegevens rapporteren. Bij niet-naleving wordt een bronheffing van 30 % toegepast op inkomsten uit Amerikaanse activa. De spreker benadrukt dat FATCA extraterritoriaal werkt: de Verenigde Staten leggen via nationale wetgeving verplichtingen op aan banken en staten buiten hun eigen jurisdictie. Dit leidde destijds tot aanzienlijke juridische weerstand, met name in Europa, waar gegevensoverdracht niet mogelijk was zonder rekening te houden met nationale privacywetgeving.

Om die juridische knoop te ontwarren creëerden de VS twee modellen van *Intergovernmental Agreements* (IGA's). Model 1 voorziet dat de banken rapporteren aan hun nationale overheid, die vervolgens de gegevens doorstuurt naar de IRS. Model 2 laat toe dat banken rechtstreeks aan de IRS rapporteren, mits instemming van hun overheid. België kiest in april 2014 voor een IGA Model 1, dat formeel wederkerigheid inhoudt: de VS zouden in theorie ook informatie over Belgische rekeninghouders in de Verenigde Staten doorgeven. De heer Van Quickenborne merkt echter op dat deze reciprociteit in de praktijk zeer beperkt blijkt en kondigt aan dat hij hierover een schriftelijke vraag aan de minister zal richten.

Na ondertekening van het FATCA-akkoord op 23 april 2014 werd het in september 2015, na vastlegging van de uitvoeringsmodaliteiten in een koninklijk besluit, volledig operationeel in België. Het kader legt Belgische financiële instellingen onder meer de verplichting op om na te gaan of hun klanten “*US indicia*” vertonen. Dat kan het bezit van een Amerikaans paspoort zijn, maar even goed een Amerikaans geboorteland, een Amerikaans adres of zelfs een telefoonnummer dat naar de VS leidt. Indien zo'n indicium aanwezig is, moet de klant zijn fiscale status bevestigen via “*self-certification*”. Wanneer blijkt dat het om een “*US person*” gaat, moeten de betrokken rekeninggegevens jaarlijks worden gerapporteerd aan de FOD Financiën, die deze vervolgens doorstuurt naar de IRS – conform het door België gekozen Model 1.

Voor elke Amerikaanse belastingplichtige omvat de rapportering minstens de naam, het adres, het Amerikaanse TIN-nummer, het rekeningnummer, het saldo op 31 december en de inkomsten uit rente, dividenden en andere activa. Deze gegevens worden elektronisch aangeleverd in een XML-formaat dat strikt beantwoordt aan de door de IRS opgelegde technische standaarden.

principe: lorsque le nouvel ambassadeur américain en Belgique ouvre un compte dans une banque, celle-ci doit constater qu'il s'agit d'un ressortissant américain, puis communiquer les données relatives à son compte. En cas de non-respect de cette obligation, les revenus provenant d'actifs américains détenus par la banque concernée font l'objet d'un prélèvement à la source à hauteur de 30 %. L'intervenant souligne l'extraterritorialité de la loi FATCA: les États-Unis imposent, par le biais de leur législation nationale, des obligations aux banques et aux États situés en dehors du territoire soumis à leur juridiction. Cela avait suscité une opposition juridique considérable à l'époque, notamment en Europe, où le transfert de données devait respecter la législation nationale en matière de protection de la vie privée.

Pour résoudre ce problème juridique, les États-Unis ont créé deux modèles d'accords intergouvernementaux (AIG). Le modèle 1 prévoit que les banques fassent rapport à leur autorité nationale, qui transmet ensuite les données à l'IRS. Le modèle 2 permet aux banques de faire directement rapport à l'IRS, moyennant l'accord de l'autorité dont elles relèvent. En avril 2014, la Belgique a opté pour un AIG de modèle 1, qui implique une réciprocité formelle: cela signifie en théorie que les États-Unis doivent également transmettre des informations sur les ressortissants belges titulaires de comptes aux États-Unis. M. Van Quickenborne fait toutefois observer que cette réciprocité est très limitée en pratique, et il annonce qu'il posera une question écrite au ministre à ce sujet.

Signé le 23 avril 2014, l'accord FATCA est pleinement entré en vigueur en Belgique en septembre 2015, après la définition de ses modalités d'exécution par arrêté royal. Ce cadre impose notamment aux établissements financiers belges de vérifier si leurs clients présentent des indices de liens avec les États-Unis (*US indicia*): possession d'un passeport américain, mais aussi naissance aux États-Unis, adresse de résidence américaine, voire numéro de téléphone avec indicatif américain. En présence d'un indice de cette nature, le client doit confirmer son statut fiscal par le biais d'une auto-certification (*self-certification*). S'il s'avère qu'il s'agit d'un contribuable américain, les données bancaires concernées devront être communiquées chaque année au SPF Finances, qui les transmettra ensuite à l'IRS, conformément au modèle 1 choisi par la Belgique.

Pour chaque contribuable américain, cette déclaration comprend au moins son nom, son adresse, son numéro fiscal américain (numéro TIN), son numéro de compte, le solde du compte concerné au 31 décembre et ses revenus provenant d'intérêts, de dividendes et d'autres actifs. Ces données sont fournies électroniquement dans un format XML qui répond strictement aux normes techniques imposées par l'IRS.

De FOD Financiën fungeert in dit systeem als “intermediaire autoriteit”: de administratie verzamelt de gegevens van alle Belgische financiële instellingen, controleert de vormvereisten en bezorgt vervolgens de volledige dataset aan de Amerikaanse belastingdienst. Theoretisch ontvangt België in ruil informatie over Belgen met rekeningen in de Verenigde Staten, maar volgens de spreker blijft deze wederzijdse uitwisseling in de praktijk bijzonder beperkt.

De privacywaarborgen onder FATCA zijn volgens hem vergelijkbaar met die van CRS: de gegevens mogen uitsluitend voor fiscale doeleinden worden gebruikt, vallen onder de Belgische gegevensbeschermingswetgeving van 2018, kennen een bewaartermijn van vijf jaar en staan onder toezicht van de GBA.

Daarna schakelt de spreker over naar de relatie tussen FATCA en het CAP. Hij benadrukt dat het CAP geen internationale rapporteringstool is, maar een nationaal identificatieregister. Het dient om binnenlandse overheidsinstanties – onder strikte voorwaarden – toe te laten na te gaan bij welke financiële instellingen een persoon rekeningen of contracten aanhoudt. FATCA daarentegen creëert een internationale rapporteringsstroom, maar beperkt tot Amerikaanse belastingplichtigen. Beide systemen functioneren volgens hem dus op verschillende niveaus van fiscale transparantie: CAP op het nationale niveau (“interne transparantie”), FATCA op het internationale (“externe transparantie”). Ze zijn complementair maar niet overlappend.

In de praktijk bestaan er procedurele raakvlakken. Wanneer Belgische banken bepalen welke rekeningen onder FATCA-rapportering vallen, doen zij dat op basis van hun klantendossiers, die deels gebaseerd zijn op informatie die ook onder het CAP-kader verplicht wordt bijgehouden. De FOD Financiën kan het CAP gebruiken om na te gaan of de banken hun FATCA-verplichtingen volledig naleven. In geval van twijfel kan de administratie via het CAP bevestigen dat een rekening daadwerkelijk bestaat en wie de titularis is. Het CAP fungeert dus als controle-instrument voor de volledigheid en juistheid van FATCA-rapportering.

Hij gaat vervolgens in op de verschillen in juridische status. FATCA rust op een internationaal verdrag in combinatie met de IGA; het CAP is louter nationaal recht. In de hiërarchie van rechtsnormen – verwijzend naar de artikelen 34 en 167 van de Grondwet – primeert de FATCA-IGA op de nationale CAP-wet. Ook het beheer verschilt: de FOD Financiën staat in voor de uitvoering van FATCA, terwijl het CAP wordt beheerd door de Nationale Bank van België. De doeleinden lopen uiteen: FATCA dient het Amerikaanse fiscale toezicht, het CAP

Dans ce système, le SPF Finances fait office d’“autorité intermédiaire”: il collecte les données de tous les établissements financiers belges, vérifie les exigences de forme et transmet ensuite l’ensemble des données à l’administration fiscale américaine. En théorie, la Belgique reçoit, en contrepartie, des informations à propos des Belges qui possèdent des comptes aux États-Unis, mais selon l’intervenant, cet échange réciproque reste très limité en pratique.

L’intervenant considère que les garanties de confidentialité prévues par l’accord FATCA sont comparables à celles du CRS: les données ne peuvent être utilisées qu’à des fins fiscales, relèvent du champ d’application de la législation belge de 2018 sur la protection des données, peuvent être conservées durant cinq ans et sont placées sous le contrôle de l’APD.

L’intervenant aborde ensuite la relation entre la FATCA et le PCC. Il souligne que le PCC n’est pas un outil de rapportage international, mais un registre d’identification national. Il sert à permettre aux autorités publiques nationales – dans des conditions strictes – de vérifier auprès de quels établissements financiers une personne détient des comptes ou des contrats. La FATCA, en revanche, crée un flux de rapportage international, mais qui se borne aux contribuables américains. Selon le membre, les deux systèmes opèrent donc à des niveaux différents de transparence fiscale: le PCC au niveau national (“transparence interne”), la FATCA au niveau international (“transparence externe”). Ces dispositifs sont complémentaires, mais ne se chevauchent pas.

En pratique, il existe des similitudes procédurales. Lorsque des banques belges déterminent quels comptes sont soumis au rapportage FATCA, elles le font sur la base de leurs dossiers clients, qui reposent en partie sur des informations qui doivent aussi être conservées dans le cadre du PCC. Le SPF Finances peut utiliser le PCC pour vérifier si les banques respectent pleinement leurs obligations relatives à la FATCA. En cas de doute, l’administration peut confirmer via le PCC qu’un compte existe effectivement et qui en est le titulaire. Le PCC sert donc d’instrument de contrôle pour vérifier l’exhaustivité et l’exactitude du rapportage FATCA.

Le membre aborde ensuite les différences en matière de statut juridique. La FATCA repose sur un traité international assorti d’un AIG, tandis que le PCC relève uniquement du droit national. Dans la hiérarchie des normes juridiques – en vertu des articles 34 et 167 de la Constitution –, l’AIG relatif à la FATCA prime la loi nationale PCC. La gestion diffère également: le SPF Finances est responsable de la mise en œuvre de la FATCA, tandis que le PCC est géré par la Banque nationale de Belgique. Leurs objectifs divergent également: la FATCA

dient de binnenlandse identificatie voor de Belgische fiscus en andere hiertoe gemachtigde overheidsdiensten.

Qua gegevensinhoud legt hij uit dat het CAP identificatie- én saldodata bevat voor binnenlandse rekeningen, terwijl FATCA vooral informatie bevat over Amerikanen met buitenlandse tegoeden. De toegang tot beide systemen is exclusief voorbehouden aan bevoegde overheidsinstanties, nooit aan het publiek.

De heer Van Quickenborne gaat vervolgens over tot een bespreking van de complementariteit tussen FATCA en het CAP in de praktijk. Hoewel beide systemen reeds inhoudelijk en procedureel met elkaar in verband zijn gebracht, benadrukt hij dat complementariteit een andere dimensie betreft dan loutere samenhang. Concreet stelt hij dat de FOD Financiën het CAP op drie manieren gebruikt in het kader van FATCA. Ten eerste dient het CAP om te verifiëren of de FATCA-rapportering van de banken effectief alle relevante rekeningen omvat. Ten tweede ondersteunt het CAP de administratie bij buitenlandse informatieverzoeken afkomstig van de IRS. Ten derde helpt het CAP vermijden dat Belgische burgers dubbel worden gerapporteerd in internationale uitwisselingsprocedures. Het CAP fungeert dus als een nationaal referentiepunt dat toelaat internationale rapportering correct, volledig en proportioneel te laten verlopen.

Daarna plaatst hij FATCA en het CAP in een constitutioneel en mensenrechtelijk kader. Beide systemen houden een inmenging in in het privéleven en dus in het recht op privacy, maar de intensiteit verschilt. Het CAP registreert vooral identificatiegegevens en saldi, terwijl FATCA inhoudelijke financiële gegevens verwerkt, wat een zwaardere inmenging vormt. Dat verschil speelt volgens hem een belangrijke rol in de proportionaliteitsbeoordeling. Het CAP is immers “getrapt” en doelgebonden: toegang is pas mogelijk wanneer er aanwijzingen van belastingontduiking bestaan én wanneer de belastingplichtige niet wenst mee te werken. FATCA daarentegen werkt systematisch: alle klanten worden op *US-indicia* gescreend, ongeacht individueel vermoeden.

Wanneer men deze gegevensverwerking toetst aan de voorwaarden uit het Valentijnsarrest van het Grondwettelijk Hof (14 februari 2013), zo vervolgt hij, moet FATCA strenger worden beoordeeld dan het CAP, net omdat de inmenging intensiever is en de proportionaliteit bijgevolg nauwer moet worden bewaakt. Het arrest verduidelijkt

sert à permettre aux autorités américaines de réaliser le contrôle fiscal, tandis que le PCC sert à permettre aux fisc belge et aux autres services publics habilités à cet effet de procéder à l'identification des comptes sur le plan national.

S'agissant du contenu des données, l'intervenant explique que le PCC contient des données d'identification et de solde pour les comptes nationaux, tandis que la FATCA contient principalement des informations sur les Américains disposant d'avoirs à l'étranger. L'accès aux deux systèmes est réservé exclusivement aux autorités publiques habilitées à cet effet, et jamais au grand public.

M. Van Quickenborne aborde ensuite la complémentarité entre la FATCA et le PCC en pratique. Bien que ces deux systèmes aient déjà été interconnectés sur le plan du contenu et de la procédure, il souligne que la complémentarité revêt une autre dimension que la seule cohésion. Concrètement, il indique que le SPF Finances utilise le PCC de trois manières dans le cadre de la FATCA. Premièrement, le PCC sert à vérifier si le rapportage FATCA des banques comprend effectivement tous les comptes pertinents. Deuxièmement, le PCC soutient l'administration dans le cadre des demandes d'informations étrangères émanant de l'IRS. Troisièmement, le PCC contribue à éviter que les citoyens belges fassent l'objet d'un double rapportage dans le cadre des procédures internationales d'échange d'informations. Le PCC fait donc office de point de référence national permettant un rapportage international correct, exhaustif et proportionnel.

L'intervenant poursuit en analysant la FATCA et le PCC à la lumière de la Constitution et des droits de l'homme. Ces deux systèmes impliquent une ingérence dans la vie privée et portent donc atteinte au droit à la vie privée, mais l'intensité de cette atteinte diffère. Le PCC enregistre surtout des données d'identification et des soldes, tandis que la FATCA traite des données financières substantielles, ce qui constitue une plus grande ingérence. Selon le membre, cette différence joue un rôle majeur dans l'examen de la proportionnalité. Le PCC est en effet “graduel” et ciblé: l'accès n'est possible que s'il existe des indications d'évasion fiscale et que si le contribuable refuse de coopérer. Le FATCA fonctionne pour sa part de manière systématique: tous les clients sont screenés à l'aune de critères baptisés *US indicia*, qu'il existe des soupçons individuels ou non.

Si l'on examine ce traitement des données à la lumière des conditions énoncées dans l'arrêt de la Saint-Valentin de la Cour constitutionnelle (arrêt du 14 février 2013), la FATCA doit être évaluée de manière plus stricte que le PCC, justement parce que son ingérence est plus grande et que sa proportionnalité doit donc être surveillée de

dat slechts een inmenging die wettelijk is, strikt noodzakelijk is en voldoende waarborgen tegen misbruik bevat, grondwettelijk standhoudt.

Aansluitend bespreekt hij de democratische legitimiteit. Het CAP is door het Parlement aangenomen en onderworpen aan grondwettelijke controle; FATCA daarentegen vloeide voort uit een internationale overeenkomst die destijds weinig parlementair debat kende. Dat roept volgens hem terechte vragen op over de democratische legitimiteit van extraterritoriale verplichtingen die door een buitenlandse staat aan Belgische instellingen worden opgelegd. De IGA-modellen hebben dat probleem slechts gedeeltelijk opgevangen.

Vervolgens schetst hij de relatie tussen FATCA, CRS en het CAP. FATCA, stelt hij, is in feite de blauwdruk voor de CRS-standaard die nadien door de OESO is ontwikkeld. CRS is multilateraal, wederkerig en veel breder opgezet dan het Amerikaanse systeem. België past vandaag drie niveaus van fiscale transparantie toe: het nationale niveau via het CAP, het bilaterale niveau via FATCA en het multilaterale niveau via CRS. Die drie systemen vormen samen een coherente piramide: CAP voor binnenlandse detectie, FATCA voor bilaterale rapportering en CRS voor multilaterale uitwisseling. Het CAP is daarin de basislaag, aangezien het de fiscus toelaat te weten welke rekeningen bestaan en welke onder FATCA of CRS vallen.

De spreker komt vervolgens tot een beleidsmatige en grondwettelijke beoordeling. Onder de sterktes vermeldt hij dat het CAP de internationale verplichtingen versterkt zonder zelf verder te gaan dan strikt noodzakelijk. FATCA verhoogt België's betrouwbaarheid als internationale partner – een positie die volgens hem niet zonder gevolgen kan worden opgegeven. Samen versterken beide systemen de traceerbaarheid van geldstromen en de effectiviteit van fraudebestrijding.

Tegelijk identificeert hij drie risico's. Ten eerste is FATCA unilateraal en asymmetrisch: gegevensstromen richting de VS zijn aanzienlijk, terwijl de wederkerigheid beperkt is. Ten tweede leidt het systeem tot hoge compliancekosten voor banken, doordat zowel FATCA- als CRS-rapportering vereist is. Ten derde bestaat er een risico op *"data mixing"* of *"function creep"*: de verleiding om gegevens uit CAP, FATCA en CRS toch met elkaar te verbinden, met potentieel zware gevolgen voor privacy en rechtsbescherming. Hij verwijst daarbij naar eerdere opmerkingen hierover van de heer Vereeck.

Op basis van dezelfde proportionaliteitslogica uit het Valentijnsarrest benadrukt hij opnieuw de nood

plus près. Cet arrêt précise que seule une ingérence légale, strictement nécessaire et assortie de garanties suffisantes contre les abus est constitutionnelle.

Il évoque dans la foulée la question de la légitimité démocratique. Le PCC a été adopté par le Parlement et soumis au contrôle constitutionnel; la FATCA, en revanche, est issue d'un accord international qui n'a fait l'objet que de peu de débats parlementaires à l'époque. Selon le membre, cela soulève des questions pertinentes quant à la légitimité démocratique d'obligations extraterritoriales imposées par un État étranger aux institutions belges. Les modèles AIG n'ont que partiellement résolu ce problème.

L'intervenant décrit ensuite la relation entre la FATCA, le CRS et le PCC. Il indique que la FATCA a en réalité servi de modèle à la norme CRS élaborée par la suite par l'OCDE. Le CRS est multilatéral, réciproque et nettement plus large que le système américain. La Belgique applique aujourd'hui trois niveaux de transparence fiscale: le niveau national via le PCC, le niveau bilatéral via le FATCA et le niveau multilatéral via le CRS. Ces trois systèmes forment ensemble une pyramide cohérente: le PCC pour la détection au niveau national, la FATCA pour le rapportage bilatéral et le CRS pour l'échange multilatéral. Le PCC en constitue la base, car il permet à l'administration fiscale de savoir quels comptes existent et lesquels relèvent de la FATCA ou du CRS.

L'intervenant procède ensuite à une évaluation politique et constitutionnelle. Parmi les forces du PCC, il mentionne que celui-ci renforce les obligations internationales sans aller au-delà de ce qui est strictement nécessaire. La FATCA renforce la fiabilité de la Belgique en tant que partenaire international, une position à laquelle, à ses yeux, elle ne pourra pas renoncer sans conséquences. Ensemble, les deux systèmes renforcent la traçabilité des flux financiers et l'efficacité de la lutte contre la fraude.

Parallèlement, il identifie trois risques. Premièrement, la FATCA est unilatérale et asymétrique: les flux de données vers les États-Unis sont considérables, tandis que la réciprocité est limitée. Deuxièmement, ce système entraîne des coûts de mise en conformité élevés pour les banques, car il exige à la fois des rapportage FATCA et CRS. Troisièmement, il existe un risque de mélange de données ou de détournement de la finalité: la tentation de recouper entre elles les données du PCC, de la FATCA et du CRS, avec des conséquences potentiellement graves pour le respect de la vie privée et la protection juridique. Il renvoie à cet égard aux observations formulées précédemment par M. Vereeck à ce sujet.

Sur la base de la même logique de proportionnalité que celle de l'arrêt de la Saint-Valentin, il souligne à

aan een trapsgewijze structuur: een eerste laag via CAP-identificatie, een tweede laag via FATCA- of CRS-rapportering, en een derde laag van gebruik onder toezicht van wettelijke waarborgen. Integratie van deze databanken tot één doorzoekbaar geheel zou volgens hem onmogelijk de proportionaliteitstoets doorstaan.

Daaruit vloeien verschillende beleidsaanbevelingen voort. Hij pleit voor het behoud van de strikte scheiding tussen CAP, FATCA en CRS, aangezien elk systeem een eigen doel en rechtsbasis heeft. Daarnaast vraagt hij om versterkte parlementaire controle op de FATCA-uitwisselingen, met onder meer een jaarlijks verslag over volumes, fouten en klachten. De louter individuele controlerechten waar parlementsleden gebruik van kunnen maken, leiden er immers toe dat bepaalde informatie nooit systematisch in het Parlement wordt gepresenteerd.

Als derde aanbeveling vraagt hij dat de proportionaliteit van de FATCA-screening wordt geëvalueerd, zeker in het licht van de GDPR die sinds 2018 nieuwe normen introduceert. Verder suggereert hij dat België diplomatiek aandringt op effectieve wederkerigheid, bijvoorbeeld tijdens toekomstige contacten met de nieuwe Amerikaanse ambassadeur. Tot slot herhaalt hij dat het CAP moet worden gebruikt als verificatietool, niet als instrument voor datamining of gedragsprofilering.

Hij sluit af met een bredere beschouwing over het evenwicht tussen internationale samenwerking en nationale rechtsbescherming. FATCA heeft volgens hem het mondiale paradigma inzake fiscale gegevensuitwisseling ingrijpend gewijzigd. België heeft die norm geïntegreerd zonder zijn constitutionele waarborgen op te geven, precies dankzij de rol van het CAP als onafhankelijk en passief register. Zolang dit register geen proactieve analysetool wordt, blijft het juridische evenwicht behouden. Volgens de heer Van Quickenborne vormt het CAP de constitutionele buffer die het mogelijk maakt internationale verplichtingen na te leven zonder dat de Belgische rechtsstaat zijn soevereine waarborgen prijsgeeft.

De heer Van Quickenborne verwijst naar zijn eerdere opmerkingen over de relatie tussen de Amerikaanse FATCA-regeling (*Foreign Account Tax Compliance Act*) en het Centraal Aanspreekpunt (CAP) bij de Nationale Bank van België. Hij verklaart dat deze beschouwing hem in de gelegenheid stelt om terug te grijpen naar een aantal kaderteksten die hij heeft voorbereid. Daarbij plaatst hij

nieuw de noodzaak van een structuur op meerdere niveaus: een eerste niveau gebaseerd op de identificatie PCC, een tweede niveau gebaseerd op het rapportage FATCA of CRS, en een derde niveau gebaseerd op de gebruik van gegevens onder de controle van wettelijke garanties. Volgens hem, de integratie van deze bankgegevens in een unieke verzameling raadpleegbaar zou niet bestand zijn tegen de controle van proportionaliteit.

Er zijn afgeleid verschillende beleidsaanbevelingen. De interveniënt pleit voor het behoud van een strikte scheiding tussen de PCC, de FATCA en de CRS, aangezien elk systeem een eigen doel en rechtsgrond heeft. Daarnaast vraagt hij om te versterken de parlementaire controle op de FATCA-uitwisselingen, met onder meer een jaarlijks verslag over de volumes, de fouten en de klachten. De louter individuele controle rechten waar de leden van het parlement gebruik van kunnen maken, leiden er immers toe dat bepaalde informatie nooit systematisch in het Parlement wordt gepresenteerd.

Als derde aanbeveling vraagt hij dat de proportionaliteit van de FATCA-screening wordt geëvalueerd, zeker in het licht van de GDPR die sinds 2018 nieuwe normen introduceert. Verder suggereert hij dat België diplomatiek aandringt op effectieve wederkerigheid, bijvoorbeeld tijdens toekomstige contacten met de nieuwe Amerikaanse ambassadeur. Tot slot herhaalt hij dat het CAP moet worden gebruikt als verificatietool, niet als instrument voor datamining of gedragsprofilering.

Hij sluit af met een bredere beschouwing over het evenwicht tussen internationale samenwerking en nationale rechtsbescherming. FATCA heeft volgens hem het mondiale paradigma inzake fiscale gegevensuitwisseling ingrijpend gewijzigd. België heeft die norm geïntegreerd zonder zijn constitutionele waarborgen op te geven, precies dankzij de rol van het CAP als onafhankelijk en passief register. Zolang dit register geen proactieve analysetool wordt, blijft het juridische evenwicht behouden. Volgens de heer Van Quickenborne vormt het CAP de constitutionele buffer die het mogelijk maakt internationale verplichtingen na te leven zonder dat de Belgische rechtsstaat zijn soevereine waarborgen prijsgeeft.

De heer Van Quickenborne verwijst naar zijn eerdere opmerkingen over de relatie tussen de Amerikaanse FATCA-regeling (*Foreign Account Tax Compliance Act*) en het Centraal Aanspreekpunt (CAP) bij de Nationale Bank van België. Hij verklaart dat deze beschouwing hem in de gelegenheid stelt om terug te grijpen naar een aantal kaderteksten die hij heeft voorbereid. Daarbij plaatst hij

de discussie in een ruimer internationaal fiscaal kader, met name dat van de FATCA, de Common Reporting Standard (CRS) en het door de OESO ontwikkelde BEPS-programma (*Base Erosion and Profit Shifting*).

Hij herinnert eraan dat het BEPS-initiatief na de financiële crisis van 2008 tot stand is gekomen, op verzoek van de G20, met als doel de uitholling van de belastinggrondslag en de kunstmatige winstverschuiving door multinationale ondernemingen tegen te gaan. De spreker schetst dat multinationals vóór de crisis hun belastingdruk aanzienlijk konden verlagen door winsten te verschuiven naar rechtsgebieden met lage of geen belastingheffing. Vanuit een liberaal perspectief stelt hij dat fiscale concurrentie tussen landen in beginsel een gezonde prikkel kan zijn voor economische groei en innovatie, maar hij erkent dat de internationale gemeenschap destijds de noodzaak inzag van een meer coherent en transparant fiscaal kader.

Vervolgens licht hij toe dat het BEPS-programma, sinds zijn lancering door de OESO in 2013, de basis vormt van een geïntegreerde wereldwijde fiscale hervorming. Het streeft naar meer coherentie in de internationale belastingregels, het principe *substance over form* en een versterking van de transparantie. Deze doelstellingen hebben geleid tot verschillende Europese en Belgische maatregelen, waaronder de *Anti-Tax Avoidance Directives* (ATAD), de reeks *Directives on Administrative Cooperation* (DAC) en de implementatie van Pillar 2, die een minimumbelasting van 15 % voor multinationale ondernemingen invoert. De heer Van Quickenborne verwijst naar de lopende omzetting van deze richtlijnen in Belgisch recht en merkt op dat België volgens experts nog niet volledig operationeel is voor de toepassing van de nieuwe aangifteplichten.

Hij komt vervolgens tot de kern van zijn betoog: de rol van het CAP binnen het BEPS-geheel. Het CAP, zegt hij, vervult een ondersteunende maar essentiële rol als juridisch veilige identificatielaag. Het biedt de administratie inzicht in rekeninghouders en maakt gerichte controles mogelijk zonder het bankgeheim volledig op te heffen. Volgens de spreker bestaat er een duidelijke parallellie tussen BEPS en het CAP, aangezien beide kaders gebaseerd zijn op transparantie, rechtmatigheid en proportionaliteit.

De heer Van Quickenborne bespreekt de drie fundamentele problemen waarop BEPS antwoorden heeft willen bieden: grondslaguitholling via renteaftrek, royalty's of hybride instrumenten; winstverschuiving naar laagbelaste jurisdicties, onder meer door transfer pricing-praktijken; en een gebrek aan transparantie, doordat

discussion dans le cadre fiscal international plus large de la FATCA, de la NCD (norme commune de déclaration) et du programme BEPS (concernant l'érosion de la base d'imposition et le transfert des bénéfices) développé par l'OCDE.

Le membre rappelle que l'initiative BEPS est née à la suite de la crise financière de 2008, à la demande du G20, en vue de lutter contre l'érosion de la base d'imposition et contre le transfert artificiel de bénéfices par les entreprises multinationales. Il explique qu'avant la crise, les multinationales pouvaient réduire considérablement leur pression fiscale en transférant des bénéfices vers des juridictions où l'imposition est faible voire nulle. D'un point de vue libéral, il estime que la concurrence fiscale entre les pays peut, en principe, constituer un stimulant sain pour la croissance économique et l'innovation, mais il reconnaît que la communauté internationale a pris conscience, à l'époque, de la nécessité d'un cadre fiscal plus cohérent et plus transparent.

L'intervenant indique ensuite que, depuis son lancement par l'OCDE en 2013, le programme BEPS est à la base d'une réforme fiscale mondiale intégrée. Ce programme vise à accroître la cohérence entre les règles fiscales internationales, à appliquer le principe de la prééminence de la substance sur la forme et à renforcer la transparence. Ces objectifs ont débouché sur plusieurs mesures au niveau belge et européen, dont les directives sur la lutte contre l'évasion fiscale (ATAD), la série de directives relatives à la coopération administrative dans le domaine fiscal (DAC) et la mise en œuvre du Pilier 2, qui instaure un impôt minimum de 15 % pour les entreprises multinationales. M. Van Quickenborne signale que ces directives sont en cours de transposition en droit belge et que, d'après les experts, la Belgique n'est pas encore totalement prête sur le plan opérationnel à appliquer les nouvelles obligations de déclaration.

Il en vient ensuite au cœur de son intervention: le rôle du PCC au sein de l'ensemble BEPS. L'intervenant indique que le PCC remplit un rôle auxiliaire mais essentiel en tant que dispositif d'identification juridiquement sécurisé. Il permet à l'administration d'avoir accès à l'identité des titulaires de comptes et de mener à bien des contrôles ciblés, sans lever l'intégralité du secret bancaire. D'après l'intervenant, il existe un parallèle évident entre le BEPS et le PCC dans la mesure où les deux cadres sont basés sur la transparence, la légitimité et la proportionnalité.

M. Van Quickenborne aborde les trois problèmes fondamentaux auxquels le principe BEPS a voulu répondre: l'érosion de la base d'imposition par la déduction des intérêts, des royalties ou des instruments hybrides; le transfert de bénéfices vers des juridictions à la taxation plus légère, notamment par l'application de pratiques de

belastingadministraties onvoldoende over accurate informatie beschikken. Het BEPS-programma omvatte vijftien concrete acties, gegroepeerd rond drie pijlers: coherentie van regels; *substance and value creation*; en transparantie en rechtszekerheid. In 2019 werd het uitgebreid met het zogenaamde BEPS 2.0-kader, waarin Pillar 1 en Pillar 2 zijn opgenomen.

De spreker geeft vervolgens een overzicht van de Europese omzetting van deze maatregelen via de ATAD- en DAC-richtlijnen en van de Belgische implementatie via onder meer de wet van 2017 en de wet van 2023 inzake de minimumbelasting (Pillar 2). Deze maatregelen versterken volgens hem de transparantie-architectuur waarin het CAP functioneel past.

De heer Van Quickenborne verduidelijkt de praktische complementariteit tussen BEPS en het CAP aan de hand van concrete voorbeelden. Bij de beoordeling van de aanwezigheid van een vaste inrichting in België kan het CAP nagaan of er Belgische rekeningen bestaan op naam van buitenlandse entiteiten. In het kader van transfer pricing kan het CAP helpen bij de identificatie van betrokken Belgische ondernemingen. Ook bij meldingsplichtige constructies onder DAC 6 of bij de inning van top-upbelastingen onder Pillar 2 kan het CAP als gericht hulpmiddel worden ingezet. Volgens hem vormen BEPS-rapportering en CAP-gegevens samen een meerschallig detectiesysteem dat internationale macrosignalen koppelt aan nationale microverificaties.

De spreker benadrukt het belang van de juridische en grondwettelijke waarborgen die aan deze systemen ten grondslag liggen. Zowel BEPS-maatregelen als het CAP steunen op formele wettelijke basissen en voldoen aan de beginselen van legaliteit, doelbinding en proportionaliteit, zoals onder meer bevestigd door het arrest van het Grondwettelijk Hof van 14 februari 2013. Het CAP wordt slechts geraadpleegd bij een concreet vermoeden van fraude en vormt dus geen instrument voor algemene dataverwerking of profilering. De heer Van Quickenborne waarschuwt uitdrukkelijk tegen pogingen om CAP-gegevens te koppelen aan algoritmische analyses of grootschalige datamining, aangezien dit in strijd zou zijn met de geest van artikel 22 van de GDPR en het grondwettelijke proportionaliteitsbeginsel.

Met betrekking tot het toezicht en de governance preciseert hij dat de Nationale Bank van België instaat voor het technisch beheer van het CAP, dat de Federale Overheidsdienst Financiën bevoegd is voor het fiscaal gebruik, en dat de Gegevensbeschermingsautoriteit extern toezicht uitoefent. Het parlement vervult de democratische

transfer pricing et un manque de transparence empêchant les administrations fiscales de disposer de toutes les informations nécessaires. Le programme BEPS énumérait quinze actions concrètes, réunies au sein de trois piliers: cohérence des règles; substance et création de valeurs; et transparence et sécurité juridique. En 2019, le programme a été élargi au cadre "BEPS 2.0", dans lequel ont été intégrés les Piliers 1 et 2.

L'intervenant donne ensuite un aperçu de la transposition européenne de ces mesures par les directives ATAD et DAC et de leur intégration en Belgique, notamment par la loi de 2017 et la loi de 2023 relative à l'impôt minimum (Pilier 2). D'après lui, ces mesures renforcent l'architecture de transparence dans laquelle s'applique le PCC.

M. Van Quickenborne illustre la complémentarité existant entre le programme BEPS et le PCC à l'aide d'exemples concrets. Lors de l'évaluation de la présence d'un établissement stable en Belgique, le PCC peut vérifier si des comptes belges ont été ouverts au nom d'entités étrangères. Dans le cadre du *transfer pricing*, le PCC peut contribuer à l'identification des entreprises belges concernées. Le PCC peut également être utilisé comme outil ciblé dans le cadre des constructions soumises à obligation de déclaration au titre de la DAC 6 ou pour la perception d'impôts complémentaires dans le cadre du Pilier 2. Selon lui, les rapports BEPS et les données du PCC forment conjointement un système de détection à plusieurs niveaux, qui associe les signaux macroéconomiques internationaux aux vérifications micro-nationales.

L'intervenant souligne l'importance des garanties juridiques et constitutionnelles sous-tendant ces systèmes. En effet, les mesures anti-BEPS et le PCC reposent sur des bases légales formelles et respectent les principes de légalité, de limitation des finalités et de proportionnalité, comme le confirme notamment l'arrêt du 14 février 2013 de la Cour constitutionnelle. Le PCC n'est consulté qu'en cas de présomption concrète de fraude et ne constitue donc pas un outil destiné à permettre le traitement généralisé des données ou le profilage. M. Van Quickenborne met expressément en garde contre toute tentative visant à soumettre les données du PCC à des analyses algorithmiques ou à du *data mining* à grande échelle, ce qui serait contraire à l'esprit de l'article 22 du RGPD et au principe constitutionnel de proportionnalité.

S'agissant du contrôle et de la gouvernance, l'intervenant précise que la Banque nationale de Belgique est chargée de la gestion technique du PCC, que le Service public fédéral Finances est habilité à utiliser le PCC à des fins fiscales et que l'Autorité de protection des données exerce un contrôle externe. Le Parlement

controlefunctie. De spreker stelt voor om jaarlijks een CAP-auditverslag op te maken met kwantitatieve en kwalitatieve indicatoren, zoals het aantal raadplegingen, de doorlooptijd en het aantal klachten, om zo de transparantie en het publieke vertrouwen te versterken.

De heer Van Quickenborne gaat vervolgens over tot een evaluatie in de vorm van een SWOT-analyse. Hij identificeert als sterktes de combinatie van BEPS-conformiteit met rechtsbescherming, het evenwicht tussen efficiëntie en privacy en het getrapte toegangsmechanisme dat *function creep* voorkomt. Als zwaktes wijst hij op de overlap tussen verschillende transparantiekaders (zoals DAC 4, DAC 6 en CAP), de beperkte publieke rapportering over hun interactie en de dreiging van datamining onder het mom van efficiëntie. Als kansen vermeldt hij de mogelijkheid om CAP-verificatie te integreren in de Pillar 2-administratie zonder extra privacy-inmenging en het gebruik van anonieme CAP-statistieken voor beleidsdoeleinden. De voornaamste bedreiging ziet hij in de verleiding om via het *money control*-concept de proportionaliteit van het systeem te ondergraven.

Daaruit leidt hij enkele beleidsaanbevelingen af. Ten eerste stelt hij voor het CAP structureel te verankeren in de BEPS-governance, bijvoorbeeld via de federale beleidsnota Financiën. Ten tweede pleit hij voor het behoud van de getrapte toegang en verzet hij zich tegen enige fusie van CAP-gegevens met internationale BEPS-databases. Ten derde vraagt hij een versterking van de parlementaire controle. Ten vierde pleit hij voor een betere technische interoperabiliteit en voor duidelijke standaarden inzake beveiligde zoekopdrachten tussen BEPS- en CAP-applicaties. Ten slotte benadrukt hij de nood aan opleiding en een ethische code voor gegevensintegriteit bij de fiscale controleurs.

De spreker besluit dat België, zolang het CAP beperkt blijft tot identificatie- en verificatiefuncties en geen analytische rol krijgt, de BEPS-doelstellingen kan uitvoeren zonder zijn democratische rechtsgrond te ondermijnen. Hij beschouwt het Belgische model als een evenwichtige combinatie van transparantie en privacy, die als best practice kan dienen binnen de OESO.

De heer Van Quickenborne vervolgt zijn uiteenzetting en richt zich op de rol van de Europese instellingen en het toezicht op de financiële datastromen. Hij wijst erop

remplit sa fonction de contrôle démocratique. L'intervenant propose d'établir chaque année un rapport d'audit sur le PCC, qui inclurait des indicateurs quantitatifs et qualitatifs comme le nombre de consultations, le délai de procédure et le nombre de plaintes reçues, en vue de renforcer la transparence et la confiance du grand public.

M. Van Quickenborne procède ensuite à une évaluation sur le modèle d'une analyse SWOT. Concernant les forces, il épingle la combinaison de la conformité des règles anti-BEPS et de la protection juridique, l'équilibre entre l'efficacité et le respect de la vie privée, ainsi que le mécanisme d'accès graduel pour prévenir tout détournement d'usage (*function creep*). Concernant les faiblesses, il souligne le chevauchement entre plusieurs cadres visant à garantir la transparence (comme les directives DAC 4 et 6 et le PCC), le rapportage public restreint à propos de leur interaction et la menace posée par le *data mining* sous prétexte d'efficacité. Concernant les opportunités, le membre mentionne la possibilité d'intégrer la consultation du PCC dans l'administration liée au Pilier 2 sans ingérence supplémentaire dans la vie privée, ainsi que l'utilisation de statistiques anonymisées du PCC à des fins politiques. Selon lui, la principale menace réside dans la tentation de saper la proportionnalité du système en recourant au *money control*.

Le membre déduit plusieurs recommandations stratégiques de ce qui précède. Premièrement, il propose de conférer un ancrage structurel au PCC dans la gouvernance relative au BEPS, par exemple au travers de la note de politique fédérale Finances. Deuxièmement, il préconise le maintien de l'accès graduel, et il s'oppose à toute fusion entre les données du PCC et celles des bases de données internationales relatives au BEPS. Troisièmement, il demande un renforcement du contrôle parlementaire. Quatrièmement, il préconise une meilleure interopérabilité technique et la définition de standards clairs en matière de recherches sécurisées entre les applications liées au BEPS et au PCC. Enfin, il souligne l'importance de prévoir, pour les contrôleurs fiscaux, des formations et un code d'éthique pour l'intégrité des données.

Le membre conclut en indiquant qu'aussi longtemps que le PCC se cantonnera à des fonctions d'identification et de vérification et ne jouera aucun rôle analytique, la Belgique pourra concrétiser les objectifs fixés en matière de BEPS sans saper son fondement démocratique. Il considère le modèle belge comme une combinaison équilibrée de transparence et de respect de la vie privée, qui pourrait servir de bonne pratique au sein de l'OCDE.

M. Van Quickenborne poursuit son exposé en s'intéressant au rôle des institutions européennes et à la surveillance des flux de données financières. Il souligne que

dat drie instellingen hierbij een sleutelrol spelen: de Europese Rekenkamer, de *European Data Protection Board* (EDPB) en de nieuwe *Anti-Money Laundering Authority* (AMLA).

Hij herinnert eraan dat de Europese Rekenkamer niet enkel de wettigheid en efficiëntie van de Europese middelen controleert, maar ook nagaat hoe de lidstaten Europese richtlijnen uitvoeren. In een rapport uit 2022 over de Europese antiwitwasbeleid, dat verscheen toen hij minister van Justitie was, werd België geciteerd als voorbeeld van *good governance* en *full audit traceability*. De spreker merkt op dat dit een positief element was binnen de toenmalige regering, en dat België door zijn gestructureerde gegevensbeheer een referentiepositie binnen de Europese Unie innam.

Vervolgens bespreekt hij de EDPB, de instantie die de toepassing en interpretatie van de GDPR binnen de Europese Unie coördineert. De EDPB publiceerde een richtsnoer over financiële interoperabiliteit waarin wordt benadrukt dat de uitwisseling van rekeninginformatie enkel toelaatbaar is op grond van een duidelijke wettelijke basis en onder toezicht van onafhankelijke autoriteiten. De heer Van Quickenborne vermeldt dat de Belgische Gegevensbeschermingsautoriteit actief heeft bijgedragen aan de totstandkoming van deze richtlijn en dat het Belgische CAP-model daarbij als referentie heeft gediend voor het concept van functionele onafhankelijkheid van gegevensverwerking.

Als derde instelling bespreekt hij de AMLA, die in 2024 in Frankfurt am Main werd opgericht en vanaf 2026 operationeel zal zijn. De AMLA krijgt onderzoeksbevoegdheden, toegang tot registers en kan sancties opleggen bij ernstige tekortkomingen. België heeft er volgens hem op aangedrongen dat de nationale parlementen hun controlebevoegdheden behouden. Artikel 21 van de AMLA-verordening bevestigt dat lidstaten hun interne toezichtmechanismen blijven beheren. Hij verwijst naar de besprekingen in de Raad van ministers, waarin België heeft beklemtoond dat Europees toezicht legitiem is, maar de nationale verantwoordelijkheid niet mag neutraliseren. Met de komst van de AMLA zal er een systeem van supranationale audits worden ingevoerd, waarbij nationale registers jaarlijks een gestandaardiseerd auditrapport aan AMLA moeten bezorgen.

De heer Van Quickenborne gaat vervolgens in op de technische interoperabiliteit en de gegevensstromen

trois institutions jouent un rôle clé à cet égard, à savoir la Cour des comptes européenne, le Comité européen de la protection des données (CEPD) et la nouvelle Autorité de lutte contre le blanchiment de capitaux et le financement du terrorisme (ALBC).

L'intervenant rappelle que la Cour des comptes européenne a non seulement pour mission de contrôler la légalité et l'efficacité de l'utilisation des fonds européens, mais aussi de vérifier comment les États membres de l'UE mettent en œuvre les directives européennes. Dans un rapport de 2022 sur la politique européenne en matière de lutte contre le blanchiment d'argent, publié alors que le membre était ministre de la Justice, la Belgique a été citée en exemple pour sa bonne gouvernance et pour le système de *full audit traceability* mis en place, ce qui était encourageant pour le gouvernement de l'époque, la Belgique occupant ainsi une position de référence au sein de l'Union européenne grâce à sa gestion des données structurée.

L'intervenant évoque ensuite le CEPD, l'instance qui coordonne l'application et l'interprétation du RGPD au sein de l'Union européenne. Le CEPD a publié une ligne directrice relative à l'interopérabilité financière, dans laquelle il souligne que l'échange d'informations concernant les comptes n'est acceptable que s'il s'appuie sur une base légale claire et a lieu sous la surveillance d'autorités indépendantes. M. Van Quickenborne indique que l'Autorité de protection des données belge a activement contribué à l'élaboration de cette directive et que le modèle de PCC belge a servi de référence à cet égard pour le concept d'indépendance fonctionnelle du traitement des données.

L'intervenant cite ensuite la troisième institution, l'ALBC, qui a été créée en 2024 à Francfort-sur-le-Main et qui sera opérationnelle à partir de 2026. L'ALBC disposera de pouvoirs d'enquête, aura accès aux registres et pourra imposer des sanctions en cas de manquements graves. Selon l'intervenant, la Belgique a insisté pour que les parlements nationaux conservent leur pouvoir de contrôle. L'article 21 du règlement relatif à l'ALBC confirme que les États membres continueront à gérer leurs mécanismes de surveillance internes. L'intervenant renvoie aux discussions menées au sein du Conseil des ministres, au cours desquelles la Belgique a souligné que la surveillance européenne est légitime, mais qu'elle ne peut pas neutraliser la responsabilité nationale. La création de l'ALBC entraîne la mise en place d'un système d'audits supranationaux dans le cadre duquel les registres nationaux devront remettre chaque année un rapport d'audit standardisé à cette institution.

M. Van Quickenborne aborde ensuite la question de l'interopérabilité technique et des flux de données au

binnen de Europese Unie. Hij verwijst eerst naar het *Common Communication Network* (CCN), het beveiligde communicatienetwerk van de Europese Commissie voor de uitwisseling van fiscale en financiële gegevens tussen de lidstaten. Dit netwerk, beheerd door DG TAXUD, maakt gebruik van end-to-end-encryptie en garandeert een minimale transmissietijd. De spreker onderstreept dat integratie met het CCN essentieel is om duplicatie van gegevens te vermijden en dat de kerninformatie tussen lidstaten automatisch wordt gesynchroniseerd.

Daarnaast verwijst hij naar het *European Financial Data Model* (EFDM), dat gebaseerd is op bestaande ISO-normen en de IBAN-structuur. Dit model beoogt een semantisch compatibel gegevenskader dat automatische vertaling en grensoverschrijdende verificatie van dataintegriteit mogelijk maakt. In dat verband vermeldt hij ook de eIDAS 2.0-verordening, die de digitale identiteit binnen de Europese Unie harmoniseert. Hierdoor zullen buitenlandse belastingautoriteiten in de toekomst via hun nationale digitale identiteitsmiddelen toegang krijgen tot specifieke gegevens, onder toezicht van AMLA. Dit gebeurt volgens het principe van *Mutual Recognition Without Data Duplication*, waarbij identiteiten wederzijds worden erkend zonder bijkomende gegevensdeling.

De spreker gaat vervolgens in op de gevolgen van deze Europese dataruimte, die volgens hem belangrijke juridische en politieke vragen oproept. Ten eerste stelt hij dat de integratie van financiële data de balans tussen nationale soevereiniteit en Europese coördinatie onder druk zet. Voor België blijft het uitgangspunt duidelijk: het CAP is en blijft een nationale databank met Europese verplichtingen, niet omgekeerd. Deze juridische afbakening bepaalt of Belgische burgers onder direct Europees toezicht vallen of enkel via hun nationale overheid. België verdedigt het principe van subsidiariteit: Europa mag coördineren, maar de lidstaten blijven eigenaar van hun gegevens.

Een tweede aandachtspunt betreft de democratische controle. De AMLA zal audits kunnen uitvoeren bij nationale registers, maar de rapportering gebeurt in eerste instantie aan de Europese instellingen. België heeft in de Raad van ministers van de Europese Unie gepleit voor het systematisch bezorgen van een kopie van de auditverslagen aan de nationale parlementen, zodat Europees toezicht gepaard gaat met nationale democratische verantwoording. Dit principe werd ook erkend in een overweging van de AMLA-verordening.

sein de l'Union européenne. Il fait d'abord référence au *Common Communication Network* (CCN), le réseau de communication sécurisé de la Commission européenne pour l'échange de données fiscales et financières entre les États membres. Ce réseau, géré par la DG TAXUD, utilise un chiffrement de bout en bout et garantit un temps de transmission minimal. L'intervenant souligne que l'intégration avec le réseau CCN est essentielle pour éviter la duplication des données et garantir la synchronisation automatique des informations clés entre les États membres.

Il évoque ensuite le *European Financial Data Model* (EFDM), qui repose sur les normes ISO existantes et sur la structure IBAN. Ce modèle vise à créer un cadre de données sémantiquement compatible, permettant la traduction automatique et la vérification transfrontalière de l'intégrité des données. À ce propos, il mentionne également le règlement eIDAS 2.0, qui harmonise l'identité numérique au sein de l'Union européenne. À l'avenir, les autorités fiscales étrangères auront ainsi accès à certaines données via leurs moyens d'identification numérique nationaux, sous la supervision de l'Autorité européenne de lutte contre le blanchiment d'argent (*Anti-Money-Laundering Authority* – AMLA). Cette procédure s'appuie sur le principe de *Mutual Recognition Without Data Duplication*, selon lequel les identités sont reconnues mutuellement sans partage supplémentaire de données.

Pour suivre, l'intervenant aborde les conséquences de cet espace européen des données, qui soulève selon lui d'importantes questions juridiques et politiques. Il souligne d'abord que l'intégration des données financières met sous pression l'équilibre entre souveraineté nationale et coordination européenne. Pour la Belgique, le principe est clair: le PCC reste une base de données nationale soumise à des obligations européennes, et non l'inverse. Cette délimitation juridique détermine si les citoyens belges sont directement soumis à un contrôle européen ou seulement à celui des autorités nationales. La Belgique défend le principe de subsidiarité: l'Europe peut coordonner, mais les États membres restent propriétaires de leurs données.

Un deuxième point d'attention concerne le contrôle démocratique. L'AMLA pourra réaliser des audits auprès des registres nationaux, mais les rapports seront d'abord transmis aux institutions européennes. La Belgique a plaidé, au sein du Conseil de ministres de l'Union européenne, pour que des copies des rapports d'audit soient systématiquement envoyées aux parlements nationaux, afin que le contrôle européen s'accompagne d'une responsabilité démocratique nationale. Ce principe a également été reconnu dans un considérant du règlement AMLA.

De heer Van Quickenborne bespreekt vervolgens de kwestie van privacy en proportionaliteit. Naarmate de gegevensuitwisseling binnen de Europese Unie uitbreidt, neemt het risico toe dat persoonsgegevens buiten hun oorspronkelijke doel worden verwerkt. Zowel de Belgische Gegevensbeschermingsautoriteit als de EDPB pleiten daarom voor het principe van *functional separation*: gegevens mogen enkel worden gebruikt voor het doel waarvoor ze zijn verzameld. Hij verwijst naar een gezamenlijk advies van 2023 waarin werd gesteld dat centralisatie geen doel op zich mag zijn, maar enkel een middel ter bevordering van efficiëntie onder rechtsstatelijke controle.

Om zijn betoog te illustreren, verwijst de spreker naar twee praktijkvoorbeelden. Het eerste betreft het project Benelux Datalink, een samenwerking tussen België, Nederland en Luxemburg met steun van de Europese Commissie. Dit project beoogt de automatische verificatie van rekeninginformatie voor grensarbeiders en multinationale ondernemingen. Het systeem maakt het mogelijk om via het CAP na te gaan of een belastingplichtige ook rekeningen in een ander Benelux-land aanhoudt, zonder dat rekeningnummers worden gedeeld. De verificatie gebeurt via tokens en niet via ruwe data, wat het model tot een voorbeeld maakt van privacy preserving interoperability. In 2024 werd het project bekroond met de *EU Good Governance Award* voor innovatieve gegevensbescherming.

Het tweede voorbeeld betreft Operation Amberline, een gecoördineerd onderzoek naar btw-carrouselfraude in vier lidstaten. Dankzij de koppeling tussen het CAP en btw-aangiften kon België binnen enkele uren de betrokken rekeningen identificeren en relevante informatie delen met Europol en het *European Anti-Fraud Office* (OLAF). De analyse leidde tot de ontwikkeling van het *European Financial Intelligence Exchange Framework* (EFICS). Beide voorbeelden tonen volgens hem aan dat Europese samenwerking niet noodzakelijk centralisatie vergt: federale interoperabiliteit – autonome systemen met gedeelde standaarden – kan even doeltreffend zijn als supranationale databanken.

De heer Van Quickenborne besluit deze passage met een reflectie over de toekomst van de Europese financiële dataruimte. Hij stelt dat de Europese Commissie sinds 2022 werkt aan de *Financial Data Space*, onderdeel van de *European Data Strategy*, die veilige en gestandaardiseerde toegang tot financiële data moet waarborgen voor zowel publieke als private instellingen. In dit model fungeert het CAP als de federale node binnen een

M. Van Quickenborne aborde ensuite la question de la vie privée et de la proportionnalité. À mesure que l'échange de données s'étend au sein de l'Union européenne, le risque augmente que certaines données à caractère personnel soient traitées à des fins autres que celles pour lesquelles elles ont été collectées. Tant l'Autorité belge de protection des données que l'EDPB plaident dès lors pour le principe de séparation fonctionnelle (*functional separation*), qui ne permet d'utiliser les données que pour l'objectif ayant justifié leur collecte. L'intervenant renvoie à un avis conjoint de 2023 selon lequel la centralisation ne peut pas constituer une fin en soi, mais ne peut être qu'un moyen de favoriser l'efficacité, sous le contrôle de l'état de droit.

Pour illustrer son propos, l'intervenant donne deux exemples pratiques. Le premier concerne le projet Benelux *Datalink*, fruit d'une coopération entre la Belgique, les Pays-Bas et le Luxembourg soutenue par la Commission européenne. Ce projet porte sur la vérification automatique des informations relatives aux comptes détenus par les travailleurs frontaliers et les entreprises multinationales. Ce système permet de vérifier, au moyen du PCC, si un contribuable détient également des comptes dans un autre pays du Benelux, sans toutefois que les coordonnées de ces comptes soient transmises. Cette vérification a lieu au moyen de *tokens* et non de données brutes, ce qui fait de ce modèle un exemple d'interopérabilité respectueuse de la vie privée. En 2024, ce projet a été récompensé par le *EU Good Governance Award* pour cette innovation en matière de protection des données.

Le second exemple de l'intervenant concerne l'opération *Amberline*, c'est-à-dire une enquête coordonnée sur la fraude carrousel à la TVA dans quatre États membres. En reliant le PCC et les déclarations TVA, la Belgique a pu, en quelques heures, identifier les comptes concernés et partager des informations pertinentes avec Europol et l'Office européen de lutte antifraude (OLAF). Cette analyse a abouti au développement du cadre européen d'échange d'informations financières (*European Financial Intelligence Exchange Framework*, EFICS). Selon lui, ces deux exemples démontrent que la coopération européenne ne requiert pas nécessairement la centralisation: l'interopérabilité fédérale – systèmes autonomes utilisant des normes partagées – peut être aussi efficace que des banques de données supranationales.

M. Van Quickenborne conclut cette intervention par une réflexion sur l'avenir de l'espace européen des données financières. Il indique que, depuis 2022, la Commission européenne œuvre à l'aménagement de l'*Espace des données financières*, qui fait partie intégrante de la *Stratégie européenne pour les données*, qui doit garantir un accès sûr et standardisé aux données financières tant pour les institutions publiques que

Europese cloudinfrastructuur: de lidstaten behouden autonomie maar delen metadata en kwaliteitsindicatoren via een centrale Europese hub.

De spreker verwijst tevens naar de *AI Act* (Verordening 2024/1391), die voorschrijft dat algoritmen die publieke gegevens verwerken, onderworpen zijn aan risicoclassificatie en menselijke controle. Voor toekomstige toepassingen van datamining of automatische profilering op CAP-gegevens acht hij deze wet van groot belang. Hij pleit ervoor dat elke vorm van automatische profilering onderworpen blijft aan menselijke en juridische toetsing.

De minister heeft twee kansen voor het grijpen. Zal hij die evenwel benutten? Vooreerst kan de inbedding van de CAP-verificatie de invordering versnellen zonder extra in te grijpen in de persoonlijke levenssfeer. Ten tweede is het mogelijk overheidsbeleidsstatistieken anoniem en dus zonder verwerking van persoonsgegevens te analyseren.

Een lichtzinnige koppeling tussen het CAP en de internationale datastromen kan leiden tot betwistingen in rechte. Bovendien kan een eventuele strategie van financiële controle (*money control* dus) het bestaansrecht van het CAP op de helling zetten.

Anders gezegd: de hele constructie dreigt dan als een kaartenhuisje in elkaar te storten.

Het is dan ook zinvol enkele aanbevelingen te doen. Zo is het raadzaam:

- het CAP structureel te verankeren in de BEPS-governancestructuur. Dat aspect kan worden opgenomen in de beleidsnota van Financiën, als instrument om de toepassing van de BEPS-regels te schragen;

- een stapsgewijze gegevenstoegang te handhaven en daarbij elke gecentraliseerde samenvoeging met de BEPS-databank uit de weg te gaan;

- voor te schrijven dat elk gebruik moet worden gemotiveerd met een welbepaald doel;

- het parlementair toezicht aan te scherpen;

- de technische interoperabiliteit te verbeteren;

- in te zetten op aangepaste opleiding en ethische bewustwording;

pour les institutions privées. Dans ce modèle, le PCC fait office de nœud fédéral au sein d'une infrastructure nuagique européenne: les États membres conservent leur autonomie mais partagent des métadonnées et des indicateurs de qualité au travers d'un *hub* central européen.

L'intervenant renvoie également au règlement sur l'IA (règlement 2024/1391), qui prévoit que les algorithmes traitant des données publiques doivent être soumis à une classification des risques et à un contrôle humain. Il estime que ce règlement revêt une grande importance pour les futures applications d'exploration ou de profilage automatique des données du PCC. Il préconise que toute forme de profilage automatique demeure soumise à un contrôle humain et juridique.

Le ministre dispose de deux opportunités qu'il devrait saisir, mais le fera-t-il? Premièrement, l'intégration de la vérification par le Point de contact central (PCC) [peut accélérer le recouvrement sans interférence supplémentaire en matière de vie privée. Deuxièmement, une analyse anonyme est possible pour les statistiques de politique publique sans traiter de données personnelles.

L'interconnexion imprudente entre le PCC et les flux de données internationaux peut entraîner des contestations juridiques. De plus une éventuelle approche de contrôle financier (*money control*) pourrait compromettre la justification du PCC.

Autrement dit, toute la construction risque de s'effondrer comme un château de cartes.

Dès lors, certaines recommandations prennent tout leur sens. Il convient ainsi:

- d'ancrer structurellement le PCC dans la gouvernance BEPS. Ce point peut être intégré dans la note de politique générale Finances en tant qu'instrument de soutien à l'application des règles BEPS;

- de maintenir un accès gradué aux données, en évitant toute fusion centrale avec la base BEPS;

- de prévoir que chaque utilisation se justifie par un objectif précis;

- de renforcer le contrôle parlementaire;

- d'améliorer l'interopérabilité technique;

- d'organiser une formation adaptée et une sensibilisation éthique;

— de integriteit van de gegevens te vrijwaren;

— het CAP-model binnen de OESO op te werpen als best practice op het gebied van nationale identificatie met eerbiediging van de grondwettelijke rechten.

Wellicht zal de minister het systeem dat hij in België bepleit niet heel vurig verdedigen binnen internationale instellingen zoals het IMF en de OESO.

De spreker geeft een samenvatting van de respectieve functies van BEPS en het CAP, die een juridisch en technisch evenwicht vormen tussen transparantie en privégegevens. België beschikt nu nog over een exemplarisch instrument.

Vervolgens analyseert de spreker het Europese kader.

Ten eerste heeft de Europese Rekenkamer België genoemd als een voorbeeld inzake *governance and full audit traceability*.

De European Data Protection Board werd opgericht bij de algemene verordening gegevensbescherming (AVG). Het Belgische CAP werd daarbij gezien als een model dat navolging verdient.

Toen de Autoriteit voor de bestrijding van witwassen en terrorismefinanciering (AMLA) werd opgericht, heeft België zich ingespannen om de rol van de nationale parlementen te behouden (zie art. 22 van Verordening (EU) 2024/1620 tot oprichting van de Autoriteit voor de bestrijding van witwassen en terrorismefinanciering).

Het beveiligde netwerk van de EU verzekert de uitwisseling van belasting- en douanegegevens tussen lidstaten (*Common Communication Network – CCN*).

De Europese Unie ontwikkelt een *EU Financial Data Model* dat verwijst naar het nieuwe Europese kader voor toegang tot financiële gegevens (FIDA – *Financial Data Access Framework*). Dat is een initiatief binnen de nieuwe EU-strategie voor digitale financiën, die tot doel heeft een gemeenschappelijk model tot stand te brengen voor het veilig delen van financiële gegevens.

Daarnaast bieden de Electronic Identification, Authentication and Trust Services (eIDAS) in de hele EU een eenvormig wettelijk kader voor de elektronische identificatie en vertrouwensdiensten.

Dit alles roept vragen op over de soevereiniteit van de lidstaten. De Europese integratie doet de vraag rijzen of de informatie nog toebehoort aan de lidstaten dan wel gemeenschappelijk wordt.

— de préserver l'intégrité des données;

— de positionner le modèle du PCC au sein de l'OCDE comme une *best practice* en matière d'identification nationale avec le respect des droits constitutionnels.

Sans doute le ministre ne plaidera pas avec grand enthousiasme au niveau international (FMI, OCDE, ...) le système qu'il prône en Belgique.

L'orateur résume les fonctions respectives du BEPS et du PCC, qui forment un équilibre juridique et technique entre la transparence et les données privées. La Belgique dispose actuellement encore d'un outil exemplaire.

Il poursuit en analysant le cadre européen.

Tout d'abord, la Cour des comptes européenne a cité la Belgique comme exemple en matière de "*governance and full audit tracability*".

Le Comité européen de la protection des données a été institué par le Règlement général sur la protection des données (RGPD). Le PCC belge a été considéré comme un modèle du genre.

Lorsque l'Autorité de lutte contre le blanchiment d'argent et le financement du terrorisme (AMLA) a été constituée, la Belgique a œuvré pour le maintien du rôle de parlements nationaux (cf. art. 22 du règlement (UE) 2024/1620 établissant l'AMLA).

Le réseau sécurisé de l'UE assure l'échange de données fiscales et douanières entre États membres (*Common Communication Network CCN*).

L'Union européenne développe un "*EU Financial Data Model*", qui renvoie au nouveau cadre européen d'accès aux données financières, appelé FIDA (*Financial Data Access Framework*). Il s'agit d'une initiative de la stratégie de finance numérique de l'UE, visant à instaurer un modèle commun de partage sécurisé des données financières.

Par ailleurs, l'*Electronic Identification, Authentication and Trust Services (eIDAS)* établit un cadre juridique uniforme dans l'UE pour l'identification électronique et les services de confiance.

Tout ceci implique des questions relatives à la souveraineté des États. L'intégration européenne au entraîne le problème de savoir si l'information appartient encore aux États ou si elle devient commune.

Voor België zijn de zaken duidelijk. Het CAP is Belgisch, maar onderworpen aan Europese verplichtingen. Het subsidiariteitsbeginsel blijft van toepassing.

Het lid wijst vervolgens op drie essentiële pijlers: de parlementaire controle, het evenredigheidsbeginsel en de bescherming van de persoonlijke levenssfeer. Hij benadrukt dat die dimensies niet los kunnen worden gezien van een nauwgezette beoordeling door de Gegevensbeschermingsautoriteit (GBA), die optreedt in coördinatie met het Europees Comité voor gegevensbescherming (EDPB). Daarbij wordt de klemtoon gelegd op het begrip “functionele scheiding”, dat een institutionele garantie vormt om de risico’s te voorkomen die gepaard gaan met een buitensporige concentratie van bevoegdheden of gegevens. Vanuit dat perspectief moet centralisatie niet worden gezien als een op zichzelf staand doel, maar als een instrument om de administratieve en operationele doeltreffendheid te vergroten, op voorwaarde dat zij omkaderd blijft door mechanismen voor controle en eerbiediging van de grondrechten.

Het lid verwijst naar het voorbeeld van de “Benelux datalink”, die werd ontwikkeld met de steun van de Europese Commissie. Dat project illustreert dat het mogelijk is een interoperabiliteitssysteem op te zetten dat de persoonlijke levenssfeer respecteert, wat werd erkend door de toekenning van de *EU Good Governance Award*. De spreker wijst er echter op dat andere ervaringen, zoals onderzoeken naar btw-carroussels in verschillende Europese landen, aantonen dat een doeltreffende samenwerking mogelijk is zonder dat gegevens systematisch worden gecentraliseerd. Die vaststelling relateert de opvatting dat supranationale gegevensbanken noodzakelijkerwijs een betere oplossing zouden zijn. De uitdaging ligt niet in de opeenstapeling van informatie, maar in de mogelijkheid een optimale coördinatie tussen de betrokken actoren te garanderen door interoperabiliteitsmechanismen te bevorderen.

In plaats van alleen maar harmonisatie te ondersteunen, zou het daarom beter zijn te evolueren naar een echte federatie. De Europese Commissie werkt momenteel aan de totstandbrenging van een Europese financiële dataruimte (*financial dataspace*), hetgeen deel uitmaakt van de bredere *European Data Strategy*. Het is de bedoeling een gemeenschappelijke infrastructuur op te zetten waarmee de lidstaten hun financiële gegevens kunnen delen, koppelen en beveiligen.

De integratie ervan met de AI Act of met de wetgeving inzake artificiële intelligentie veronderstelt menselijk toezicht. Het belang van Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 tot vaststelling van geharmoniseerde regels betreffende

Pour la Belgique, les choses sont claires. Le PCC est belge, mais est soumis à des obligations européennes. Le principe de subsidiarité demeure d’application.

Ensuite, le membre met en évidence trois axes essentiels: le contrôle parlementaire, le principe de proportionnalité et la protection de la vie privée. Il souligne que ces dimensions ne peuvent être dissociées d’une évaluation attentive menée par l’Autorité de protection des données (APD), laquelle agit en coordination avec le Comité européen de la protection des données (EDPB). L’accent est ainsi placé sur la notion de *functional separation*, qui constitue une garantie institutionnelle visant à prévenir les risques liés à une concentration excessive des pouvoirs ou des données. Dans cette perspective, la centralisation ne doit pas être appréhendée comme une finalité autonome, mais bien comme un instrument destiné à accroître l’efficacité administrative et opérationnelle, à condition qu’elle demeure encadrée par des mécanismes de contrôle et de respect des droits fondamentaux.

Le membre met en avant l’exemple du *Benelux datalink*, développé avec le soutien de la Commission européenne. Ce projet illustre la possibilité de mettre en place un système d’interopérabilité respectueux de la vie privée, reconnu par l’attribution du *EU Good Governance Award*. Toutefois, il rappelle que d’autres expériences, telles que les enquêtes menées sur les réseaux de carroussels de TVA dans plusieurs États européens, démontrent qu’une coopération efficace peut être réalisée sans recourir à une centralisation systématique des données. Cette observation conduit à relativiser l’idée selon laquelle les banques de données supranationales constitueraient nécessairement une solution supérieure. L’enjeu ne réside pas dans l’accumulation d’informations, mais dans la capacité à assurer une coordination optimale entre les acteurs concernés, en privilégiant des mécanismes d’interopérabilité.

Dès lors, au lieu de soutenir une simple harmonisation, il serait préférable d’évoluer vers une véritable fédération. La Commission européenne poursuit actuellement la mise en place d’un espace européen des données financières (*financial dataspace*), inscrit dans le cadre plus large de la *European Data Strategy*. L’objectif est de créer une infrastructure commune permettant aux États membres de partager, d’interconnecter et de sécuriser leurs données financières.

L’intégration avec la AI Act ou la loi sur l’intelligence artificielle impose un contrôle humain. L’importance de ce règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l’intelligence artificielle et

artificiële intelligentie en tot wijziging van bepaalde wetgevingshandelingen van de Unie mag niet worden onderschat (cf. *impact algorithmische beoordeling*).

Men mag ook de burger zelf niet vergeten en evenmin de initiatieven met betrekking tot het Handvest van de digitale rechten; een en ander beoogt de rechten van de burger inzake gegevens te verankeren. Het Belgisch Parlement heeft zich ten gunste van een dergelijke evolutie uitgesproken.

Eurostat heeft de economische impact van een gegevenscentralisatie onderzocht: er zou 45 miljard euro per jaar kunnen worden bespaard doordat aldus komaf wordt gemaakt met ondoelmatige procedures en de veelheid aan controles. Centralisatie roept echter ook vragen op over de macht die aldus wordt gegenereerd en over het toezicht op het informatiebeheer. Het antwoord ligt in een systeem van checks-and-balances.

Het lid sluit af met een beschrijving van hoe het beheer van de financiële gegevens in België georganiseerd is; daaruit blijkt het belang dat aan soevereiniteit wordt gehecht. Hij vervolgt met het gedetailleerde onderzoek van hoe een en ander in de Zwitserse Bondsstaat is georganiseerd (instelling van het interne klantenregister, de antiwitwaswet, het eeuwenoude bankgeheim).

Onder internationale druk heeft het land sinds 2000 een diepgaande transformatie ondergaan. Hoewel er geen formeel CAP is, garandeert het Zwitserse recht de traceerbaarheid van alle bankrekeningen. De Meldestelle für Geldwäscherei (MROS) speelt daarin een sleutelrol.

Kortom, Zwitserland streeft naar een evenwicht tussen de voor de economie noodzakelijke financiële privacy en transparantie tegenover de bevoegde autoriteiten. Tegelijk schikt het land zich naar de verwachtingen van de internationale organisaties en van andere staten. Gegevenscentralisatie is geen doel; wel wil men gebruik kunnen maken van een doeltreffend traceringsysteem in geval van vermoedens van witwaspraktijken, terrorisme of belastingontwijking.

De spreker overloopt de juridische grondslagen van de antiwitwaswet en gaat in op de werking van de federale autoriteit voor toezicht op de financiële markten (FINMA) en van de federale belastingdienst (AFC), zonder daarbij het bureau voor de melding van witwaspraktijken (MROS) over het hoofd te zien. Voormelde instellingen zijn met elkaar verbonden via een coördinatieplatform. Hij beschrijft de constitutionele structuur van de Zwitserse Bondsstaat en haar relatie met de kantons, alsook de internationale samenwerking.

modifiant certains actes législatifs de l'Union ne peut être minimisée (cf. *impact algorithmic assessment*).

Par ailleurs, il ne faut pas oublier les citoyens eux-mêmes et les initiatives relativement à la Charte des droits numériques visant à consacrer les droits des personnes en matière de données. Le Parlement belge s'est exprimé en faveur de pareille évolution.

Eurostat a analysé les effets économiques d'une centralisation des données: cela peut entraîner une économie de 45 milliards d'euro annuellement en évitant des procédures inefficaces et la multiplication des contrôles. Toutefois, la centralisation appelle aussi des questions sur le pouvoir qu'elle génère et le contrôle de la gestion de l'information. La réponse réside dans un système de freins et contrepoids.

Le membre conclut par une description de l'organisation belge, qui témoigne de l'importance accordée à la souveraineté, et passe à l'examen détaillé de l'organisation de la Confédération helvétique, avec la création du registre interne des clients et sa loi sur le blanchiment d'argent (LBA), mais aussi le secret bancaire multiséculaire.

Depuis l'an 2000, le pays a subi une transformation en profondeur à la suite de pressions internationales. Sans disposer formellement d'un PCC, le droit suisse garantit la traçabilité de tous les comptes bancaires. Le Bureau de communication en matière de blanchiment d'argent y joue un rôle essentiel.

En résumé, la Suisse vise le respect de l'équilibre entre la vie privée financière, essentielle pour l'économie, et la transparence vis-à-vis des autorités compétentes, tout en se conformant aux attentes de la part des organisations internationales et d'autres États. Le but n'est pas de centraliser l'information, mais de pouvoir bénéficier d'un système de traçabilité efficace en cas de soupçon de blanchiment d'argent, de terrorisme ou d'évasion fiscale.

Le membre parcourt les fondements juridiques de la LBA et aborde le fonctionnement de l'Autorité fédérale de surveillance des marchés financiers (FINMA) et de l'Administration fédérale des contributions (AFC), sans oublier le Bureau de communication en matière de blanchiment d'argent (MROS) – reliés par une plateforme de coordination – et décrit la structure constitutionnelle de la Confédération helvétique et sa relation avec les entités décentralisées, mais aussi la coopération internationale.

De spreker besteedt bijzondere aandacht aan de toegang tot en het beheer van informatie, maar ook aan de procedurele aspecten, alvorens de werkzaamheden van de federale functionaris voor gegevensbescherming en transparantie toe te lichten en in te gaan op de federale wet inzake gegevensbescherming, die vergelijkbaar is met Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

Het Zwitserse rechtsbestel beschikt over een robuust systeem dat willekeurige handelingen voorkomt en rekening houdt met de aanbevelingen van de FATF (*Financial Action Task Force*). Zwitserland onderscheidt zich door een sterke bescherming van persoonsgegevens en heeft de OESO-norm inzake automatische uitwisseling van fiscale inlichtingen (CRS – *Common Reporting Standard*) aangenomen, die in 2017 in werking is getreden.

Zo is het bureau voor de melding van witwaspraktijken (MROS) belast met het ontvangen en onderzoeken van vermoedens van witwaspraktijken op nationaal niveau, terwijl de federale belastingdienst (AFC) instaat voor de automatische internationale uitwisseling van fiscale inlichtingen (AEOI).

De verordening van de FINMA inzake het witwassen van geld (AMLO-FINMA) verduidelijkt dan weer de verplichtingen van de financiële tussenpersonen in Zwitserland.

Het lid citeert een aantal statistieken uit het jaarverslag 2024 van het MROS (Zwitsers meldpunt voor witwaspraktijken) en geeft een kritische bespreking van de evaluaties en implicaties voor een aantal betrokken actoren (parlement, administratie, balie, politie enzovoort).

De EU oefent grote druk uit om Zwitserland ertoe aan te zetten geharmoniseerde normen aan te nemen, hoewel het land geen lidstaat is. Het lijkt erop dat de EU haar doel bereikt, want Zwitserland is akkoord gegaan.

Op basis van de kwaliteiten van het Zwitserse systeem formuleert het lid een aantal aanbevelingen. België zou het volgende moeten doen:

- voorzien in een formele verankering door middel van een intern klantenregister, zoals in het Zwitsers recht (cf. *supra*);

- sneller toegang bieden tot de gegevens wanneer het gerecht dringendheid aanvoert;

L'intervenant accorde une attention particulière à l'accès et à la gestion de l'information, mais aussi aux aspects de procédure, avant de présenter les travaux du Préposé fédéral à la protection des données et à la transparence et d'évoquer la loi fédérale sur la protection des données (LPD), comparable au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

L'ordre juridique suisse dispose d'un système robuste qui prévient des agissements arbitraires et tient compte des recommandations du GAFI (Groupe d'action financière). La Suisse se fait remarquer par une forte protection des données privées et a adopté la norme de l'OCDE sur l'échange automatique de renseignements en matière fiscale (CRS – *Common Reporting Standard*), entrée en vigueur en 2017.

Ainsi, le Bureau de communication en matière de blanchiment d'argent (MROS) est chargé de recevoir et d'analyser les soupçons de blanchiment d'argent au niveau national, tandis que l'Administration fédérale des contributions (AFC) organise l'échange automatique international de renseignements fiscaux (AIA).

L'Ordonnance de la FINMA sur le blanchiment d'argent (AMLO-FINMA) précise, quant à elle, les obligations des intermédiaires financiers en Suisse.

Le membre livre une série de statistiques du rapport annuel 2024 du MROS (Bureau de communication en matière de blanchiment d'argent) et fournit un commentaire critique des évaluations et des implications pour une série d'acteurs concernées (le Parlement, l'administration, le barreau, la police, ...).

L'UE exerce une forte pression afin de l'inciter la Suisse à adopter des standards harmonisés, alors qu'il s'agit d'un État non membre, et il semblerait qu'elle parvienne à ses fins, puisque la Suisse a marqué son accord.

Se fondant sur les qualités du système suisse, le membre formule une série de recommandations. Il conviendrait que la Belgique:

- prévoie un ancrage formel au moyen d'un registre interne des clients tel que prévu en droit suisse (*supra*);

- offre un accès plus rapide aux données en cas d'urgence exigée par la Justice;

- de technische integratie van de databanken organiseren met behulp van een eenvormig identificatie-instrument;

- de controle op de algoritmische analyse opvoeren;

- de transparantie bevorderen door jaarlijks statistieken over het gebruik en de resultaten te publiceren.

Samengevat kan worden gesteld dat het Zwitsers systeem een uniek hybride model is dat voldoet aan internationale normen en tegelijk de kern van het bankgeheim respecteert. Het combineert federale coördinatie met juridische precisie en technische maturiteit, en bevindt zich tussen de Europese en Angelsaksische benadering van financiële transparantie in. Zwitserland bewijst dat een land waar financiële discretie heerst, efficiënte instanties kan opzetten die solide garanties bieden, op voorwaarde dat er een politieke consensus is.

Ten derde is er de politieke gevoeligheid dat bij elke uitbreiding van de MROS-bevoegdheden wordt gestoten op een debat rond privacy en het bankgeheim. Op zich is dat laatste geen beperking maar veeleer een opportuniteit. In Zwitserland blijkt men immers even kritisch te zijn als in België, en evengoed aan te sturen op een ernstig debat over de problematiek. Sinds 2020 zijn door de digitalisering de interinstitutionele beperkingen gradueel afgenomen.

Wat zijn de plannen om het systeem te moderniseren en te hervormen? Blijkbaar wil men de meldingsplicht uitbreiden naar advocaten en trustkantoren. Dat is op dit ogenblik nog niet het geval bij het CAP. Er is verder de mogelijkheid tot geautomatiseerde zoekopdrachten door justitie in spoedgevallen. En er is de wettelijke verankering van het Kontenregister.

Het Zwitserse Parlement discussieert thans over de vraag of er een centrale rekeningbank moet worden opgericht. De Zwitserse banksector verzet zich daartegen wegens de kosten en de privacyrisico's. De linkse partijen pleiten er voor meer transparantie naar Europees model. De discussie loopt dus in het land en is er op dit ogenblik nog niet beslecht.

De spreker gaat vervolgens in op de federale standpunten in Zwitserland. Het federale departement van Financiën steunt er de gematigde hervorming, met het behoud van MROS als aanspreekpunt, doch met een snellere elektronische toegang voor de politiediensten. De nationale bank van Zwitserland waarschuwt dat een te open register het vertrouwen van internationale cliënten kan ondermijnen. De *data protection commissioner*

- organise l'intégration technique des banques de données à l'aide d'un outil d'identification uniforme;

- renforce le contrôle sur l'analyse algorithmique;

- promeuve la transparence par la publication annuelle de statistiques sur l'utilisation et les résultats.

En conclusion, le système suisse se présente comme un modèle hybride unique qui répond aux normes internationales tout en respectant le cœur du secret bancaire. Il allie une coordination fédérale à la précision juridique avec une maturité technique, et se situe entre l'approche européenne et anglo-saxonne de la transparence financière. La Suisse démontre qu'un pays où règne la discrétion financière peut se doter d'organes efficaces offrant des garanties solides lorsqu'il existe un consensus politique.

Troisièmement, la sensibilité politique est telle que toute extension des compétences du MROS suscite un débat sur le respect de la vie privée et du secret bancaire. En soi, cela ne constitue pas une limitation, mais plutôt une opportunité. En Suisse, on se montre en effet aussi critique qu'en Belgique, et l'on souhaite tout autant engager un débat sérieux sur la question. Depuis 2020, la numérisation a progressivement réduit les limitations interinstitutionnelles.

Quels sont les projets de modernisation et de réforme du système? Apparemment, la Suisse souhaite étendre l'obligation de signalement aux avocats et aux bureaux fiduciaires. Ce n'est pas encore le cas actuellement pour le PCC. La Justice a par ailleurs la possibilité d'effectuer des recherches automatisées en cas d'urgence. Et la loi consacre désormais l'ancrage juridique du Registre des comptes.

Le Parlement suisse débat actuellement sur l'opportunité de créer une banque centrale des comptes. Le secteur bancaire suisse s'y oppose en raison des coûts et des risques pour la vie privée. Les partis de gauche plaident pour plus de transparence, à l'instar du modèle européen. La discussion est donc en cours dans le pays et n'est, à l'heure actuelle, pas encore tranchée.

L'intervenant aborde ensuite les positions fédérales en Suisse. Le département fédéral des Finances soutient une réforme modérée, en maintenant le MROS comme point de contact, mais avec un accès électronique plus rapide pour les services de police. La Banque nationale suisse met en garde contre le fait qu'un registre trop ouvert pourrait nuire à la confiance des clients internationaux. Le Préposé fédéral à la protection des

(EDÖB) vraagt garanties dat datamining of risicoscoring enkel op geanonimiseerde datasets gebeurt.

In het kader van het politiek en institutioneel debat in Zwitserland is er ook sprake van Europese druk. Hoewel Zwitserland geen EU-lidstaat is, oefent de Europese Unie sedert lange tijd druk uit via de AMLA-verordening om geharmoniseerde standaarden in te voeren. De Zwitserse regering heeft toegezegd dat de wetgeving zal worden aangepast om volledige compatibiliteit met de EU-vereisten inzake het CAP te verzekeren.

Wat kan op basis van het voorgaande worden besloten? Ten eerste, op het vlak van de effectiviteit wordt geconcludeerd dat het Zwitserse MROS-systeem efficiënt, juridisch solide en internationaal geloofwaardig is. Het biedt alle noodzakelijke functies van een CAP aan zonder de symboliek van het opheffen van het bankgeheim. De effectiviteit blijkt uit de snelle responstijd, de hoge rapporteringsgraad en de nauwe samenwerking met buitenlandse autoriteiten.

Ten tweede wordt inzake het beleidsevenwicht gesteld dat Zwitserland een delicaat evenwicht heeft bereikt: er is transparantie voor bevoegde autoriteiten, er is strikte privacybescherming voor burgers en er is de internationale naleving zonder aantasting van de concurrentiekracht.

Welke aanbevelingen kunnen op basis hiervan worden geformuleerd? Een eerste aanbeveling is de zorg voor een formele verankering. Het Kontenregister dient expliciet te worden opgenomen in de Geldwäschereigesetz (GwG) als centraal aanspreekpunt. Ten tweede dient sneller toegang te worden gegeven door in spoedgevallen beperkte automatische zoekfuncties toe te laten voor justitie. Ten derde wordt aanbevolen te zorgen voor de technische integratie van de databanken van MROS, ESTV en FINMA via een uniform identificatiesysteem. De vierde aanbeveling heeft betrekking op het monitoringkader. Er wordt gepleit voor een versterking van de rol van de EDÖB in het toezicht op de algoritmische analyse. Ten vijfde wordt inzake de publieke communicatie aanbevolen om de transparantie te bevorderen aan de hand van de jaarlijkse publicatie van statistieken over het gebruik en de resultaten.

Hieruit kan worden besloten dat het Zwitserse systeem een uniek hybride model vormt. Het is geen klassiek CAP zoals in België, maar is een functioneel equivalent ervan dat voldoet aan de internationale normen en tegelijk de kern van het Zwitserse bankgeheim respecteert. Het combineert federale coördinatie, juridische precisie en

gegevens en à la transparence (PFPDT) demande des garanties pour que le *data mining* ou la classification des risques s'effectue uniquement sur des ensembles de données anonymisés.

Le débat politique et institutionnel en Suisse porte aussi sur la pression européenne. Bien que la Suisse ne soit pas membre de l'Union européenne, celle-ci exerce depuis longtemps une pression via le règlement AMLA pour instaurer des normes harmonisées. Le gouvernement suisse s'est engagé à adapter la législation afin d'assurer une compatibilité totale avec les exigences de l'UE relatives au PCC.

Que peut-on conclure sur la base de ce qui précède? Premièrement, sur le plan de l'effectivité, le système MROS suisse est manifestement efficace, juridiquement solide et crédible au niveau international. Il offre toutes les fonctions nécessaires d'un PCC sans remettre symboliquement en cause le secret bancaire. L'effectivité se manifeste par la rapidité de réponse, par le taux élevé de signalement et par la coopération étroite avec les autorités étrangères.

Deuxièmement, il est constaté que la Suisse a atteint un équilibre délicat en matière politique: la transparence pour les autorités compétentes va de pair avec une protection stricte de la vie privée pour les citoyens, et le respect des normes internationales ne porte pas atteinte à la compétitivité.

Quelles recommandations peuvent être formulées sur la base de cette expérience? Premièrement, il convient de veiller à un ancrage formel. Le Registre des comptes doit être explicitement intégré en tant que point de contact central dans la loi fédérale concernant la lutte contre le blanchiment d'argent (LBA). Deuxièmement, il convient d'accélérer l'octroi de l'accès en autorisant, dans les cas urgents, des fonctions de recherche automatique limitées à des fins judiciaires. Troisièmement, il est recommandé d'assurer l'intégration technique des banques de données du MROS, de l'AFC et de la FINMA au moyen d'un système d'identification uniforme. La quatrième recommandation concerne le cadre de suivi. Il est conseillé de renforcer le rôle du PFPDT dans la surveillance de l'analyse algorithmique. Cinquièmement, en matière de communication publique, il est préconisé de promouvoir la transparence par la publication annuelle de statistiques sur l'utilisation et les résultats.

On peut en conclure que le système suisse constitue un modèle hybride unique. Il ne s'agit pas d'un PCC classique comme en Belgique, mais d'un équivalent fonctionnel qui répond aux normes internationales, tout en respectant l'essence même du secret bancaire suisse. Il combine coordination fédérale, précision juridique et

technische maturiteit en kan beschouwd worden als een brug tussen de Europese en Anglo-Amerikaanse benaderingen van financiële transparantie. Zwitserland bewijst dat zelfs binnen een traditie van financiële discretie en modern, transparant en efficiënt aanspreekpunt kan functioneren mits sterke waarborgen en politieke consensus.

De spreker gaat vervolgens in op de technische werking en de operationele structuren. Het gaat daarbij om de technische realisatie, de datastroom, de beveiliging en het toezicht die de Zwitserse autoriteiten toepassen op het systeem. Uiteraard blijft het uitgangspunt hetzelfde, met name dat er geen publiek toegankelijk register is maar een geautomatiseerd en strikt gecontroleerd informatiemechanisme waarin MROS de rol van technisch en juridisch centraal aanspreekpunt vervult.

De werking van het systeem illustreert de Zwitserse benadering van discrete efficiëntie, met een minimale gegevensverwerking en een maximale bruikbaarheid voor justitie en verdere opvolging.

De architectuur van het systeem is als volgt. Er is de technische kern, het goAML-platform. Sinds 2015 gebruikt MROS dat internationaal platform, dat werd ontwikkeld door UNODC als basisplatform voor gegevensinzameling en analyse. Het platform is modulair opgebouwd en bevat drie onderdelen: de *submission gateway* (de beveiligde ingang voor melding van banken en financiële instellingen), de *analytic database* (de relationele databank waarin de meldingen en de bijhorende klantgegevens worden opgeslagen) en er is de query- en case-management-module waarin MROS-analisten zoekopdrachten uitvoeren.

Er zijn in Zwitserland meer dan 4000 financiële tussenpersonen aangesloten op de *submission gateway* (banken, vermogensbeheerders, verzekeringsmaatschappijen, notarissen). Zij gebruiken een standaard XML-schema om verdachte transacties of rekeningopeningen te melden. Elke instelling beschikt over een uniek FINMA-identificatienummer en een digitale sleutel die door de overheid wordt uitgegeven. Het systeem ondersteunt zowel batch-uploads als single-entry portals.

Het interne datamodel is als volgt. De *analytic database* bevat per melding een aantal kernvelden (het rekeningnummer, de naam van de houder en in die van toepassing de economisch rechthebbende, de datum van opening en sluiting van de rekening, enzovoort). Transactiebedragen worden niet systematisch opgeslagen. Ze verschijnen enkel in de afzonderlijke Suspicious Transaction Reports (STR). Het Kontenregister bestaat

maturité technique et peut être considéré comme une passerelle entre les approches européenne et anglo-américaine de la transparence financière. La Suisse prouve que même dans une tradition de discrétion financière, un point de contact peut fonctionner de manière moderne, transparente et efficace, à condition de bénéficier de garanties solides et d'un consensus politique.

L'intervenant aborde ensuite le fonctionnement technique et les structures opérationnelles. Il évoque ainsi la réalisation technique, le flux de données, la sécurisation et le contrôle exercé par les autorités suisses sur le système. Bien entendu, le principe de base reste le même, à savoir qu'il n'y a pas de registre accessible au public, mais un mécanisme de communication d'informations automatisé et strictement contrôlé dans lequel le MROS sert de point de contact central, tant sur le plan technique que sur le plan juridique.

Le fonctionnement du système illustre l'efficacité discrète de l'approche suisse, qui se caractérise par un traitement minimal des données et une utilité maximale pour la justice et le suivi ultérieur.

L'intervenant s'attarde ensuite sur l'architecture du système, qui repose sur un noyau technique: la plateforme goAML. Depuis 2015, le MROS utilise cette plateforme internationale, qui a été développée par l'ONUDC comme base pour la collecte et l'analyse des données. La plateforme est modulaire et inclut trois composants: l'accès sécurisé pour le signalement des banques et des institutions financières (*submission gateway*), la banque de données relationnelle dans laquelle sont stockés les signalements et les données clients (*analytic database*) et le module *query- and case-management*, dans lequel les analystes du MROS effectuent leurs recherches.

En Suisse, plus de 4000 intermédiaires financiers (banques, gestionnaires de patrimoine, compagnies d'assurances, notaires) sont connectés à la *submission gateway*. Ils utilisent un schéma XML standard pour signaler des transactions ou ouvertures de comptes suspects. Chaque institution dispose d'un numéro d'identification FINMA unique et d'une clé numérique délivrée par les autorités. Le système gère à la fois les téléversements en lot (*batch uploads*) et les portails à entrée unique (*single-entry portals*).

Le modèle de données interne se présente comme suit. L'*analytic database* contient, pour chaque signalement, une série de champs clés (numéro de compte, nom du titulaire et, le cas échéant, du bénéficiaire économique, date d'ouverture et de fermeture du compte, etc.). Les montants des transactions ne sont pas systématiquement enregistrés. Ils n'apparaissent que dans les rapports distincts de transactions suspectes (*Suspicious*

dus in de enge zin uit metagegevens over rekeningen en niet uit financiële stromen.

Op het vlak van de rapportageprocessen en de informatiestroom is er in de eerste plaats de meldingsplicht en de gegevensoverdracht. Artikel 9 van de GwG verplicht financiële instellingen om onverwijld melding te doen van elke transactie waarvan ze vermoeden dat ze verband houdt met witwassen of de financiering van terrorisme. Deze meldingen vormen de primaire input voor MROS. Daarnaast zijn instellingen verplicht om rekeningen te registreren waarvan de houder in een meldingsdossier voorkomt, inclusief alle gelieerde rekeningen en alle gelieerde subrekeningen. De informatiestroom loopt in drie richtingen: er is de informatie van de financiële instellingen naar MROS (de verdachte transacties en rekeningmeldingen), er is de informatiestroom van MROS naar de justitiële autoriteiten (de doorgestuurde dossiers) en er zijn de dossiers tussen MROS en de buitenlandse CFI's. Elke melding krijgt een referentie en wordt gekoppeld aan een *case-ID* zodra MROS beslist dat het om een relevant dossier gaat.

Wat is de frequentie en het volume? Volgens het MROS-jaarverslag van 2024 werden er 10.456 meldingen ontvangen of gemiddeld 870 per maand. 72 % van de meldingen kwam via een geautomatiseerd rapportagekanaal (via de grote banken) en 28 % werd handmatig ingevoerd door de kleine instellingen of door niet-financiële tussenpersonen. Van de meldingen werden ongeveer 75 % afgesloten zonder gevolg en 25 % doorgestuurd naar de politie of het parket.

De interne workflow bij MMROS verloopt in vier fasen. Ten eerste is er de screeningfase, met een automatische controle op de volledigheid en de basale risicofactoren. Ten tweede is er de analysefase waarin een analist de context vergelijkt met eerdere meldingen en eventuele zoekopdrachten doet in het Kontenregister. Ten derde is er de beslissingsfase waarbij een teamleider beslist of de zaak aan justitie wordt overgemaakt. Tot slot is er de opslagfase: het dossier wordt gearhiveerd en relevante rekeningen blijven gemarkeerd voor latere referentie.

Wat is de beveiliging en de privacybescherming? Het systeem voldoet aan de veiligheidsbeveiligingsstandaarden (end-to-end-encryptie, authenticatie met digitale certificaten, segmentatie van netwerkzones en logging van alle acties). Naast de technische beveiliging

Transaction Reports – STR). Le registre des comptes se limite donc strictement à des métadonnées sur les comptes et n'inclut pas les flux financiers.

En ce qui concerne les processus de signalement et le flux d'informations, le membre évoque d'abord l'obligation de communiquer et le transfert de données. L'article 9 de la loi sur le blanchiment d'argent oblige les établissements financiers à communiquer sans délai toute transaction qu'ils soupçonnent d'être liée au blanchiment d'argent ou au financement du terrorisme. Ces communications constituent la principale source d'informations du MROS. En outre, les établissements sont tenus d'enregistrer les comptes dont le titulaire figure dans un dossier ayant fait l'objet d'une communication, y compris l'ensemble des comptes et sous-comptes liés. Les informations circulent dans trois directions: tout d'abord, des établissements financiers au MROS (les transactions suspectes et les communications de comptes), ensuite du MROS aux autorités judiciaires (les dossiers transmis) et, enfin, du MROS aux CRF étrangères. Chaque communication reçoit une référence et est associée à un numéro de dossier dès que le MROS décide qu'il s'agit d'un dossier pertinent.

En ce qui concerne la fréquence et le volume de ces communications, l'intervenant renvoie au rapport annuel 2024 du MROS, qui indique que 10.456 communications ont été reçues, soit une moyenne de 870 par mois. Par ailleurs, 72 % de ces communications ont été transmises via un canal de signalement automatisé (par l'intermédiaire des grandes banques) et 28 % ont été saisies manuellement par de petits établissements ou par des intermédiaires non financiers. Près de 75 % de ces communications ont été classées sans suite et 25 % ont été transmises à la police ou au parquet.

Le flux opérationnel interne du MROS comprend quatre phases. La première est la phase de sélection, au cours de laquelle un contrôle automatique de l'exhaustivité des données et des facteurs de risque fondamentaux est effectué. La deuxième est la phase d'analyse, au cours de laquelle un analyste compare le contexte avec les communications antérieures et effectue d'éventuelles recherches dans le registre des comptes. La troisième est la phase de décision, au cours de laquelle un chef d'équipe décide si l'affaire doit être transmise à la justice. Enfin, la quatrième est la phase de stockage: le dossier est archivé et les comptes pertinents restent marqués pour référence ultérieure.

Qu'en est-il de la sécurité et de la protection de la vie privée? Le système répond aux normes de sécurité (chiffrement de bout en bout, authentification par certificats numériques, segmentation des zones de réseau et journalisation de toutes les actions). Outre ces mesures

is er de bescherming van de persoonsgegevens en de proportionaliteit. Omdat het Zwitserse systeem gevoelige identificatiegegevens bevat, past MROS het principe van de minimale dataverwerking toe (enkel relevante velden worden opgeslagen, automatische verwijdering van irrelevante gegevens, geanonimiseerde opslag van gesloten dossiers voor statistische doelen).

De EDÖB heeft toegang tot de beveiligingslogboeken en controleert jaarlijks of de proportionaliteit van de gegevensverwerking wordt gerespecteerd. Wat is de interne governance in het hoofdstuk beveiliging en privacybescherming? Elke medewerker van MROS heeft een persoonlijk toegangsniveau dat wordt bepaald door de functie en de senioriteit. Bij vertrek van een medewerker wordt het account onmiddellijk gedeactiveerd. Alle logbestanden blijven minstens tien jaar bewaard. Er is ook gegevensuitwisseling met andere instanties.

MROS beschikt ook over een interne auditcel van vijf medewerkers die de naleving van de procedures controleert. De audit omvat steekproeven van dossiers, de controle van rechtmatigheid van de zoekopdrachten, de naleving van bewaartermijnen en het correct gebruik van de toegangsrechten. Elk kwartaal wordt daarover gerapporteerd. Er zijn de laatste jaren geen ernstige afwijkingen gemeld. Daarnaast zijn er externe audits. De EDÖB voert bijvoorbeeld jaarlijks een privacy-audit uit.

Voorts is er de parlementaire controle. MROS, FINMA en ESTV brengen jaarlijks verslag uit over het aantal meldingen en zoekopdrachten, het gebruik van de middelen, de internationale samenwerking en de geplande verbeteringen. Een parlementaire commissie kan getuigen oproepen en aanbevelingen doen. Deze commissie vervult de rol die in EU-landen vaak aan de Europese Rekenkamer of de Europese Commissie toekomt.

Inzake technologische ontwikkelingen en innovatie kan worden opgemerkt dat MROS sinds 2021 investeert in het project goAML+, dat gebruik maakt van kunstmatige intelligentie om de meldingen te prioriteren. Het systeem analyseert historische data en berekent een alertscore. Deze score bepaalt welke dossiers mensen kan analyseren en eerst behandelen. Hoewel Zwitserland geen expliciete *datamining* op het CAP toelaat, wordt voor de operationele efficiëntie wel een gecontroleerde data-analyse uitgevoerd binnen MROS. Het verschil is principieel: de analyse dient enkel om

visant à assurer la sécurité technique, les données à caractère personnel sont protégées et le principe de proportionnalité est appliqué. Dès lors que le système suisse contient des données d'identification sensibles, le MROS applique le principe du traitement minimal des données (enregistrement des champs pertinents uniquement, suppression automatique des données non pertinentes, stockage anonymisé des dossiers clôturés à des fins statistiques).

Le PFPDT a accès aux journaux de sécurité et contrôle chaque année le respect de la proportionnalité du traitement des données. En ce qui concerne la gouvernance interne en matière de sécurité et de protection de la vie privée, chaque collaborateur du MROS dispose d'un niveau d'accès personnel qui dépend de sa fonction et de son ancienneté. Lorsqu'un collaborateur quitte l'organisation, son compte est immédiatement désactivé. Tous les fichiers journaux sont conservés pendant au moins dix ans. Un système d'échange de données avec d'autres instances a également été mis en place.

Le MROS dispose en outre d'une cellule d'audit interne composée de cinq collaborateurs chargés de contrôler le respect des procédures. L'audit comprend des contrôles aléatoires de dossiers, la vérification de la légalité des recherches, le respect des délais de conservation et l'utilisation correcte des droits d'accès. Un rapport est établi chaque trimestre à ce sujet. Aucune anomalie grave n'a été signalée ces dernières années. Des audits externes sont également réalisés. Le PFPDT effectue par exemple chaque année un audit sur la protection de la vie privée.

Un contrôle parlementaire est par ailleurs exercé. Le MROS, la FINMA et l'AFC font rapport chaque année sur le nombre de signalements ("communications" dans la législation suisse) et de recherches, l'utilisation des ressources, la coopération internationale et les améliorations prévues. Une commission parlementaire peut convoquer des témoins et formuler des recommandations. Cette commission remplit le rôle qui, dans les pays de l'Union européenne, incombe souvent à la Cour des comptes européenne ou à la Commission européenne.

En matière de développements technologiques et d'innovation, il convient de noter que depuis 2021, le MROS investit dans le projet goAML+, qui utilise l'intelligence artificielle pour hiérarchiser les signalements. Le système analyse les données historiques et calcule un score d'alerte. C'est sur la base de ce score que sont sélectionnés les dossiers à analyser et à traiter en priorité par les collaborateurs. Bien que la Suisse n'autorise pas explicitement le *data mining* sur les données du PCC, une analyse contrôlée des données est effectuée au sein du MROS pour améliorer l'efficacité opérationnelle. La

interne werkprocessen te optimaliseren en niet om burgers of bedrijven proactief te profileren. In de technologische ontwikkeling en innovatie is ook veel aandacht voor blockchain en digitale activa. Zo kunnen crypto-activa in verband worden gebracht met traditionele financiële stromen. Deze technologische integratie toont de vooruitstrevende aard van het Zwitserse model. Het blijft binnen het kader van financiële privacy, maar omarmt tegelijkertijd nieuwe analysetechnieken.

De volgende verbeteringen worden nog gepland: de automatische validatie van meldingen, de federale interoperabiliteit tussen MROS en de kantonale parketten en *real-time alerts* voor dringende witwasvermoedens.

Het Zwitserse systeem combineert dus technologische verfijning met juridische terughoudendheid. Het systeem verwerkt jaarlijks vele meldingen en zoekopdrachten, maar blijft volledig binnen het kader van professionaliteit en privacybescherming.

Het centraal aanspreekpunt via MROS wordt gekenmerkt door het ontbreken van een directe publieke of fiscale zoekfunctie en de aanwezigheid van een sterk toezicht aan logging, een hoog technisch beveiligingsniveau en een functionele samenwerking met een internationale service.

De heer Van Quickenborne gaat vervolgens dieper in op de analyse en het risicobeoordelingsproces. Elke melding die via het goAML-platform binnenkomt, wordt door MROS in twee fases verwerkt, met een automatische pre-analyse en een menselijke beoordeling. De pre-analyse gebruikt logische regels en beperkte patroonherkenning om meldingen te prioriteren. Het systeem kent geen volwaardige *datamining* in de betekenis van autonome patroonherkenning over het hele dataset. Algoritmen voeren enkele risicoclassificaties uit binnen de grenzen van het dossier dat wordt behandeld. Na de automatische stap volgt een dubbele beoordeling door een analist (vier-ogen-principe).

Om efficiënter te werken, hanteert MROS sinds 2022 een intern model dat gebaseerd is op het risiconiveau. Er wordt ook gebruik gemaakt van interne kennisdatabanken.

Het Zwitserse model is opzettelijk conservatief in zijn gegevensgebruik. Massale correlaties of voorspellende modellen zijn niet toegestaan omdat zij het proportionaliteitsbeginsel zouden schenden. In plaats daarvan

différence est fondamentale: l'analyse sert uniquement à optimiser les processus de travail internes et non à profiler proactivement les citoyens ou les entreprises. Dans le domaine du développement technologique et de l'innovation, une grande attention est également accordée à la blockchain et aux actifs numériques. Les crypto-actifs peuvent ainsi être mis en relation avec les flux financiers traditionnels. Cette intégration technologique illustre le caractère avant-gardiste du modèle suisse, qui respecte le principe de la confidentialité des données financières tout en adoptant de nouvelles techniques d'analyse.

Les améliorations suivantes sont encore prévues: la validation automatique des signalements, l'interopérabilité fédérale entre le MROS et les parquets cantonaux et les alertes en temps réel concernant les suspicions de blanchiment d'argent qui requièrent une action urgente.

Le système suisse allie donc sophistication technologique et retenue juridique. Il traite chaque année de nombreuses communications et requêtes, tout en respectant pleinement les principes de professionnalisme et de protection de la vie privée.

Le point de contact central géré par le MROS se caractérise par l'absence d'une fonction de recherche publique ou fiscale directe et un contrôle strict de la journalisation, par un niveau de sécurité technique élevé et par une coopération fonctionnelle avec un service international.

M. Van Quickenborne aborde ensuite en détail l'analyse et le processus d'évaluation des risques. Chaque signalement reçu au travers de la plateforme goAML est traité par le MROS en deux phases, à savoir d'abord une préanalyse automatisée et ensuite une évaluation humaine. La préanalyse utilise des règles logiques et une reconnaissance de modèles limitée pour hiérarchiser les signalements. Le système n'effectue pas de véritable *data mining*, en ce sens qu'il ne procède pas à une reconnaissance autonome de modèles sur l'ensemble des données. Les algorithmes effectuent quelques classifications de risques dans les limites du dossier traité. Après cette étape automatisée, une double évaluation est effectuée par un analyste (principe des quatre yeux).

Afin de renforcer son efficacité, le MROS applique depuis 2022 un modèle interne axé sur le niveau de risque. Il utilise aussi des bases de connaissances internes.

Le modèle suisse est délibérément conservateur dans son utilisation des données. Les corrélations massives ou les modèles prédictifs ne sont pas autorisés, car ils violeraient le principe de proportionnalité. En lieu

worden regelmatig gebaseerde filters gebruikt die door de EDÖB en FINMA zijn goedgekeurd. Deze filters zijn volledig traceerbaar en ook herleidbaar.

Vervolgens wijst de spreker op de samenwerking met de banksector. In Zwitserland heeft elke bank een eigen anti-witwas unit of AML-desk. Die vormen de eerste verdedigingslinie en voeren klanten- en transactiescreenings uit. Pas wanneer een interne melding wordt goedgekeurd, gaat ze naar MROS. De structuur waarborgt dat het Kontenregister alleen kwalitatieve gegevens ontvangt en niet overladen wordt met ruis.

Er bestaat in de strijd tegen het witwassen ook een forum waarop MROS, FINMA en de Zwitserse bankenvereniging praktische richtlijnen ontwikkelen. Via dit forum worden ook nieuwe typologieën van witwassen besproken, bijvoorbeeld met betrekking tot cryptotransacties en trustconstructies. Er zijn ook feedbackmechanismen met de banksector. MROS zendt elk kwartaal geaggregeerde feedbackrapporten naar banken met informatie over het aantal meldingen dat door MROS wordt of werd afgewezen, de belangrijkste redenen voor onvolledige rapportage en nieuwe risicoindicatoren. Die cyclus heeft de kwaliteit van meldingen aanzienlijk verhoogd.

De grote banken gebruiken rechtstreeks API-koppelingen met GoAML. Zo kunnen ze meldingen verzenden en statusinformatie ontvangen zonder handmatige tussenkomst. Deze interfaces zijn gebaseerd op ISO-formaten en ondergaan sterkte veiligheidstesten door FINMA.

Voor wat betreft de internationale coördinatie en gegevensuitwisseling dient te worden gewezen op het bestaan van de Egmont Groep, waarvan MROS een actief lid is. Via het Egmont Secure Web (ESW) kan IMROS in realtime gegevens uitwisselen met andere CFI's.

Wat is de samenwerking met de EU? Ondanks het feit dat Zwitserland geen EU-lidstaat is, is het technisch aangesloten op het Europese platform. Het kan gegevens uitwisselen met de Europese autoriteiten over grensoverschrijdende witwasnetwerken. Het Zwitsers Parlement werkt aan een verdrag dat volledige interoperabiliteit tussen MROS en de toekomstige anti-witwasautoriteit van de EU moet verzekeren.

et place, des filtres basés sur des règles et approuvés par le PFPDT et la FINMA sont utilisés. Ces filtres sont entièrement traçables.

L'intervenant évoque ensuite la coopération avec le secteur bancaire. En Suisse, chaque banque dispose de sa propre unité de lutte contre le blanchiment d'argent (*AML-desk*). Ces unités constituent la première ligne de défense et procèdent à un filtrage des clients et des transactions. Ce n'est qu'une fois qu'un signalement interne est approuvé qu'il est transmis au MROS. Cette structure permet au Registre des comptes de recevoir uniquement des données qualitatives et de ne pas être surchargé d'informations inutiles.

Le MROS, la FINMA et l'Association suisse des banquiers conçoivent des directives pratiques au sein d'un forum dédié à la lutte contre le blanchiment. Les membres de ce forum discutent également des nouvelles typologies de blanchiment, en ce qui concerne notamment les transactions en crypto-actifs et les structures de trust. Il existe aussi des mécanismes de *feedback* avec le secteur bancaire. Tous les trimestres, le MROS envoie aux banques des rapports de *feedback* consolidés contenant des informations sur le nombre de signalements refusés par le MROS, les raisons principales pour lesquelles le rapportage est incomplet et les nouveaux indicateurs de risque. Ce cycle a considérablement augmenté la qualité des signalements.

Les grandes banques utilisent directement des connexions API avec GoAML. De cette façon, elles peuvent envoyer des notifications et recevoir des informations liées au statut sans que cela nécessite une intervention manuelle. Ces interfaces s'appuient sur des formats ISO et sont soumises à des tests de sécurité rigoureux de la part de la FINMA.

En ce qui concerne la coordination et l'échange de données à l'international, il convient de souligner l'existence du Groupe d'Egmont, dont le MROS est un membre actif. Par le biais de l'Egmont Secure Web (ESW), le MROS peut échanger des informations en temps réel avec d'autres CRF.

Quelle forme prend la collaboration avec l'UE? Certes, la Suisse n'est pas un État membre de l'UE, mais elle est techniquement connectée à la plate-forme européenne. Elle peut échanger des données avec les autorités européennes sur les réseaux transfrontaliers de blanchiment d'argent. Le Parlement suisse travaille à l'élaboration d'une convention devant assurer une interopérabilité complète entre le MROS et la future autorité antiblanchiment de l'UE.

Verder is er de internationale statistische rapportering. Zwitserland publiceert jaarlijks geaggregeerde cijfers aan de FATF en aan de OESO. In 2024 werden 6320 internationale verzoeken ontvangen en 5170 verzoeken beantwoord. Er was een gemiddelde responstijd van negen dagen en 95 % van de verzoeken betrof de identificatie van rekeninghouders. Deze gegevens plaatsen Zwitserland in de top vijf van de meest actieve CFI's in Europa.

Er zijn ook de operationele evaluatie en de efficiëntie-indicatoren, met het aantal meldingen die werden doorgestuurd naar de politie, de doorlooptijd en de nalevingsgraad van de banken. In 2024 ging het om 10.456 meldingen, waarvan er 4980 werden doorgestuurd naar de politie, met een gemiddelde doorlooptijd van 6 uur en een nalevingsgraad van ongeveer 99 %. De laatste jaren kan men spreken van een gestage professionalisering en digitalisering van het proces.

Er is ook de kwalitatieve impact. De Zwitserse Bondsraad stelde in zijn verslag 2025 dat het MROS-systeem de slagkracht van de Zwitserse rechtsstaat tegen financiële criminaliteit merkbaar heeft verhoogd. Belangrijke resultaten zijn de snellere identificatie van rekeningstructuren bij BTW-fraude, een betere traceerbaarheid van crypto-stromen en een hogere interne compliance in de banksector.

Wat zijn de kritieken en de uitdagingen? Er blijven drie punten van zorg. Ten eerste gaat het om de federale versnippering van het systeem: kantons hebben verschillende protocollen voor rechtshulp. De rechtshulp is met andere woorden kantonaal georganiseerd, waarbij dus elk kanton verdragen dient te sluiten met het buitenland. Ten tweede is er de beperkte toegang. De Zwitserse justitie vraagt dan ook een snellere rechtstreekse toegang tot rekeninginformatie. Ten derde is er de politieke weerstand tegen meer automatisering. De Zwitserse bankenvereniging verzet zich met name tegen het uitbreiden van de algoritmische analyse. De Bondsraad onderzoekt momenteel een fast-track-procedure voor urgente zaken met behoud van toezicht door de EDÖB.

Wat zijn de toekomstige ontwikkelingen en aanbevelingen? Er is vooreerst een conceptwet voor de herziening van de GwG. Die herziening zal Zwitserland nader brengen bij de EU-praktijk, zonder het bankgeheim volledig op te heffen.

De strategie *Digital Finance Integrity 2025-2030* voorziet in (1) de migratie naar een federale cloud met

Ensuite, l'intervenant cite le rapportage statistique international. Tous les ans, la Suisse communique des chiffres consolidés au GAFI et à l'OCDE. En 2024, 6.320 demandes internationales ont été reçues, dont 5.170 ont reçu une réponse. Le temps de réponse moyen était de neuf jours et 95 % des requêtes portaient sur l'identification de titulaires de compte. Ces chiffres placent la Suisse dans le top cinq des CRF les plus actives en Europe.

L'intervenant cite encore l'évaluation opérationnelle et les indicateurs d'efficacité, parmi lesquels le nombre de signalements transférés à la police, la durée de traitement et le taux de conformité des banques. En 2024, on a enregistré 10.456 signalements, dont 4.980 ont été transférés à la police, avec une durée de traitement moyenne de 6 heures et un taux de conformité d'environ 99 %. Ces dernières années, on peut parler d'une professionnalisation et d'une numérisation progressives du processus.

Il y a aussi l'impact qualitatif. Dans son rapport 2025, le Conseil fédéral suisse a indiqué que le système MROS avait largement renforcé la capacité d'action de l'État de droit suisse face à la criminalité financière. Parmi les résultats importants figurent l'augmentation de la rapidité d'identification des structures de comptes en cas de fraude à la TVA, une meilleure traçabilité des flux crypto et une augmentation de la conformité interne dans le secteur bancaire.

Quelles critiques ont été émises et quels défis restent à relever? Trois points d'inquiétude subsistent. Premièrement, le système est fragmenté selon un modèle fédéral: les cantons appliquent différents protocoles pour l'aide juridique. En d'autres termes, l'aide juridique est organisée au niveau des cantons, chacun d'entre eux devant conclure des traités avec l'étranger. Deuxièmement, l'accès reste limité. La justice suisse demande dès lors un accès direct plus rapide aux informations liées aux comptes. Troisièmement, les projets d'automatisation rencontrent une résistance dans le monde politique. L'association suisse des banquiers s'oppose notamment à l'élargissement de l'analyse algorithmique. Le Conseil fédéral envisage actuellement une procédure accélérée pour les affaires urgentes, tout en maintenant la surveillance du PFPDT.

Quelles sont les évolutions et les recommandations à venir? Tout d'abord, il existe un avant-projet de loi visant à réviser la LBA. Cette révision rapprochera la Suisse de la pratique de l'UE, sans lever complètement le secret bancaire.

La stratégie *Digital Finance Integrity 2025-2030* prévoit (1) la migration vers un cloud fédéral accompagné

AI-ondersteunende detectie van patronen, (2) meer geautomatiseerde uitwisseling tussen MROS, FINMA en ESTV en (3) de ontwikkeling van privacy-preserving technieken voor statistische analyse.

Zwitserland wil zich profileren als hub voor financiële integriteit met privacybescherming. Het doel is niet de EU-regels blind te kopiëren, maar een model aan te bieden dat efficiëntie en discretie met elkaar verzoent. Om die reden pleit de Bondsraad voor een Europees memorandum over de uitwisseling van rekeninformatie tussen EU en niet-lidstaten met gelijke privacy-standaarden. Het Kontenregister is een technologisch geavanceerd, maar juridisch behoedzaam systeem. Kenmerken ervan zijn de centrale coördinatie via MROS met een strikte toegang, een hoog niveau van digitale veiligheid en proportionaliteit, een beperkt getoetst gebruik van data-analyse, een intensieve samenwerking met de banksector en internationale CFI's en een duidelijke richting naar modernisering en Europese convergentie. Zwitserland bewijst dat een Staat met een sterke privacy-traditie toch een volwaardig en efficiënt aanspreekpunt kan onderhouden dat de doelstelling van financiële transparantie en witwasbestrijding volledig ondersteunt.

Er is ook een luik over de effectiviteit en de beleidsevaluatie. Zwitserland bevindt zich in een unieke positie. Het is geen lid van de Europese Unie, maar heeft zich vrijwillig aangesloten bij vrijwel alle relevante internationale standaarden in zaken anti-witwasbeleid en fiscale transparantie (de FATF, de Egmont Groep, de OESO, enzovoort). Daarmee balanceert het land voortdurend tussen twee beleidsdoelen, met enerzijds het behoeden van de financiële privacy als traditioneel fundament van het Zwitserse bankmodel, en anderzijds het garanderen van transparantie en samenwerking in het internationale financiële verkeer. Het Kontenregister vormt de institutionele kern van dat evenwicht.

Welke resultaten levert het Zwitserse systeem op? De jaarlijkse rapporten van MROS en van FINMA bieden een solide dataset voor effectiviteitsanalyse. De beschikbare cijfers wijzen op een stijgende efficiëntie en een hoger succespercentage in vervolging. Het systeem is dus niet alleen administratief, maar ook operationeel doeltreffend. De kwalitatieve effecten zijn er uiteraard ook. Naast kwantitatieve cijfers benadrukt MROS dat de kwaliteit van meldingen merkbaar verbeterd is: een betere identificatie van *beneficial owners*, meer contextuele informatie bij internationale geldstromen en een sterkere samenwerking met compliance-afdelingen van

d'une détection de schémas assistée par l'IA, (2) une densification des échanges automatisés entre le MROS, la FINMA et l'AFC, et (3) la conception de techniques d'analyse statistique respectueuses de la vie privée.

La Suisse nourrit l'ambition de se positionner comme un pôle d'intégrité financière assorti d'une protection de la vie privée. L'objectif n'est pas de copier aveuglément les règles européennes, mais de mettre sur pied un modèle conciliant efficacité et discrétion. Pour cette raison, le Conseil fédéral plaide pour la mise en place d'un memorandum européen sur l'échange de données liées aux comptes entre l'UE et des États non-membres appliquant les mêmes niveaux de protection de la vie privée. Le Registre des comptes est un système technologique avancé, mais conçu selon un modèle juridique prudent. Il se caractérise par la coordination centrale par l'intermédiaire du MROS avec un accès strict, un niveau élevé de sécurité numérique et de proportionnalité, une utilisation limitée et éprouvée de l'analyse des données, une collaboration intensive avec le secteur bancaire et les CRF internationales et une volonté claire de modernisation et de convergence européenne. La Suisse prouve qu'un État disposant d'une longue tradition de respect de la vie privée est malgré tout capable de maintenir un point de contact à part entière et efficace qui soutienne pleinement l'objectif de transparence financière et de lutte contre le blanchiment.

Il y a également un volet qui porte sur l'efficacité et l'évaluation des politiques. La Suisse occupe une position unique. Elle n'est pas membre de l'Union européenne, mais elle s'est ralliée, d'initiative, à presque toutes les normes internationales pertinentes en matière d'antiblanchiment et de transparence fiscale (GAFI, Groupe d'Egmont, OCDE, etc.). Le pays oscille dès lors constamment entre deux objectifs, à savoir, d'une part, préserver la confidentialité financière en tant que fondement traditionnel du modèle bancaire suisse et, d'autre part, garantir la transparence et la collaboration dans la gestion des flux financiers internationaux. Le Registre des comptes constitue le centre névralgique institutionnel de cet équilibre.

Quels sont les résultats du système suisse? Les rapports annuels du MROS et de la FINMA constituent un ensemble de données solide pour l'analyse de l'effectivité de ce système. Les chiffres disponibles montrent une efficacité croissante et un taux de réussite plus élevé des poursuites engagées. L'efficacité du système ne se cantonne donc pas au volet administratif, elle touche également le volet opérationnel. On constate bien sûr aussi des améliorations de la qualité. Le MROS souligne qu'outre une amélioration quantitative, ce modèle a également permis d'optimiser sensiblement la qualité des signalements: meilleure identification des *beneficial*

banken. Het Kontenregister fungeert daarbij als centrale schakel zodra een persoon of onderneming in meerdere meldingen voorkomt. Het systeem detecteert die overlap onmiddellijk.

De Bondsraad schat dat dankzij de verbeterde traceerbaarheid jaarlijks tussen 1,2 en 1,5 miljard Zwitserse frank aan niet-gedeclareerde vermogens of ideale opbrengsten wordt ontdekt. Hoewel slechts een fractie daarvan tot veroordelingen leidt, vormt het een substantieel afschrikkingsmechanisme.

De spreker maakt vervolgens de vergelijking met de Europese modellen en belicht de typologie van het Europese CAP-systeem. Binnen Europa kunnen drie hoofdmodellen worden onderscheiden: de centrale databanken (zoals België), de volledig gebaseerde systemen (Duitsland, Oostenrijk, Finland en Zweden bijvoorbeeld) en de hybride modellen (bijvoorbeeld Zwitserland en Luxemburg). Het Zwitserse Kontenregister behoort duidelijk tot de derde categorie. De vergelijking met België is evident. De wettelijke basis is de wet van 2018, met koninklijke besluiten van 2019 en 2020. In Zwitserland is de wettelijke basis de GwG.

In België is er qua structuur een centrale databank bij de NBB en de FOD Financiën. In Zwitserland is dat het virtuele register via MROS (goAML). In België is er een rechtstreekse toegang en via zoekopdrachten door de fiscus en de politie bij het CAP. In Zwitserland verlopen de aanvragen via de MROS-analisten. Op het vlak van de data-inhoud is er een licht verschil tussen de beide landen.

Datamining is in België toegelaten onder toezicht. Dat is het systeem *money control*. In Zwitserland is het verboden, doch enkel voor risicoclassificatie. De beheerder in België is de NBB. In Zwitserland is dat het Bundesamt für Polizei. Het toezicht wordt in België uitgeoefend door de Gegevensbeschermingsautoriteit (GBA). In Zwitserland zijn dat de EDÖB en de FINMA.

De Belgische aanpak is proactief en gericht op een snelle fiscale analyse. De Zwitserse aanpak is dan weer reactief en juridisch beperkt. Toch halen beide systemen een vergelijkbare efficiëntie in witwasopsporing.

Vervolgens betreft de spreker ook de situatie in Frankrijk. Daar geldt sinds 1982 het systeem FICOBA. Het wordt beheerd door de DGFIP (*Direction Générale*

owners, plus d'informations contextuelles concernant les flux financiers internationaux et collaboration accrue avec le département *compliance* des banques. Le Registre des comptes joue ainsi un rôle central lorsqu'une personne ou une entreprise apparaît dans plusieurs signalements. Le système détecte immédiatement ces recoupements.

Selon les estimations du Conseil fédéral, grâce à l'amélioration de la traçabilité, ce sont tous les ans entre 1,2 et 1,5 milliard de francs suisses de patrimoine non déclaré ou de revenus illégaux qui sont découverts. Certes, seule une partie des dossiers débouche sur une condamnation, mais le caractère dissuasif du mécanisme est non négligeable.

L'intervenant établit ensuite une comparaison avec les modèles européens et commente la typologie du système PCC européen. Trois modèles principaux peuvent être distingués en Europe: les banques de données centrales (comme en Belgique), les systèmes déclaratifs (comme en Allemagne, en Autriche, en Finlande et en Suède, par exemple) et les modèles hybrides (par exemple, la Suisse et le Luxembourg). Le Registre des comptes suisse relève clairement de la troisième catégorie. La comparaison avec la Belgique est évidente. Notre base légale est la loi de 2018, avec des arrêtés royaux en 2019 et 2020. En Suisse, la base légale est la LBA.

En Belgique, sur le plan structurel, la BNB et du SPF Finances disposent d'une banque de données centrale. En Suisse, il s'agit d'un registre virtuel (*goAML*) administré par le MROS. En Belgique, l'accès à la banque de données est direct, et le fisc et la police effectuent des recherches dans le PCC. En Suisse, les demandes passent par les analystes du MROS. En ce qui concerne le contenu des données, une légère différence existe entre les deux pays.

En Belgique, l'exploration de données est autorisée sous surveillance. C'est le système du *money control*. En Suisse, elle est interdite, mais uniquement pour la classification des risques. En Belgique, la BNB est le gestionnaire. En Suisse, il s'agit de l'Office fédéral de la police. En Belgique, la surveillance est exercée par l'Autorité de protection des données (APD) et, en Suisse, par le PFPDT et la FINMA.

L'approche belge est proactive et centrée sur une analyse fiscale rapide. L'approche suisse est en revanche réactive et juridiquement limitée. Ces deux systèmes ont cependant une efficacité comparable en matière de détection du blanchiment d'argent.

L'intervenant évoque ensuite la situation en France, où le système FICOBA est en vigueur depuis 1982. La DGFIP (*Direction générale des Finances publiques*) en

des Finances Publiques). FICOBA centraliseert gegevens van alle Franse banken en laat de fiscus rechtstreeks zoeken. Zwitserland heeft dezelfde technische maturiteit, maar weigert een zelfde mate van open toegang. Het verschil weerspiegelt twee cultuurmodellen: de Franse statistische logica van volledige overheidskennis tegenover de Zwitserse federalistische logica van het vertrouwens- en proportionaliteitsbeheer.

Er kan ook worden vergeleken met Duitsland en Oostenrijk. Die beide landen behouden zeer strenge privacykaders. Hun systemen verplichten banken gegevens te leveren bij een gerechtelijke aanvraag, maar verbieden een structurele opslag. Zwitserland bevindt zich tussen die posities in en behoudt de bankprivacy, maar geeft de autoriteit een snellere toegang via MROS.

De heer Van Quickenborne wijst vervolgens op de sterktes van het Zwitsers model. Vooreerst is er de juridische robuustheid. Het systeem berust op drie belangrijke pijlers. De GwG bepaalt de melding en de bewaarplicht. De Bankgesetz (bankenwet) definieert de uitzondering op het bankgeheim. De DSG verzekert de naleving van de privacyregels.

Ten tweede is er ook de institutionele consistentie. MROS functioneert als een geïntegreerde hub tussen financiële instellingen, toezichthouders en justitie. De samenwerking van FINMA en ESTV verloopt via vaste protocollen en voorkomt bevoegdheidsconflicten. Dit model van functionele centralisatie zonder institutionele fusie geldt internationaal als een voorbeeld.

Ten derde is er de technische maturiteit. De combinatie van het goAML-platform (ISO-gecertificeerd) met de federale cloud-infrastructuur maakt het systeem technologisch zeer robuust. Het kan miljoenen records per jaar verwerken met een fotomarge onder de 0,1 %. Audit- en loggingfuncties behoren tot de strengste van het Europees continent.

Ten vierde is er ook de sterkte van de internationale geloofwaardigheid, met het feit dat de wetgeving FATF-conform is, het feit dat men deelneemt aan de Egmontgroep en het feit dat men de OESO-CRS-standaard uitvoert. Daardoor geniet Zwitserland internationaal vertrouwen. Dat verklaart waarom het land sinds 2019 niet meer voorkomt op enige grijze lijst van de FATF.

est le gestionnaire. Le FICOBA centralise les données de toutes les banques françaises, et le fisc peut y effectuer des recherches sans passer par un intermédiaire. La Suisse, qui dispose de la même maturité technique, refuse d'ouvrir l'accès dans la même mesure. Cette différence reflète deux modèles culturels: la logique étatique française selon laquelle l'État doit tout savoir, face à la logique fédéraliste suisse de gestion fondée sur la confiance et la proportionnalité.

Une comparaison peut également être faite avec l'Allemagne et l'Autriche. Ces deux pays maintiennent des cadres de protection de la vie privée très stricts. Les banques y sont contraintes de communiquer des données à la demande de la justice, mais le stockage structurel y est interdit. La Suisse se situe entre ces deux positions et maintient la confidentialité bancaire, tout en donnant aux autorités un accès plus rapide au travers du MROS.

M. Van Quickenborne souligne ensuite les points forts du modèle suisse, au premier rang desquels figure sa solidité juridique. Le système repose sur trois piliers essentiels. La LBA fixe l'obligation de signalement et de conservation. La loi sur les banques définit l'exception au secret bancaire. La loi sur la protection des données assure le respect des règles en matière de protection de la vie privée.

Le modèle suisse se caractérise ensuite par sa cohérence institutionnelle. Le MROS fonctionne comme un *hub* intégrant les établissements financiers, les autorités de surveillance et la justice. La coopération avec la FINMA et l'AFC suit des protocoles fixes et évite les conflits de compétence. Ce modèle de centralisation fonctionnelle sans fusion institutionnelle est considéré comme un exemple sur le plan international.

Le troisième point fort de ce modèle est sa maturité technique. La combinaison de la plateforme goAML (certifiée ISO) et de l'infrastructure fédérale en nuage rend le système particulièrement robuste sur le plan technologique. Il peut traiter des millions d'enregistrements par an avec une marge d'erreur inférieure à 0,1 %. Les fonctions d'audit et de *logging* comptent parmi les plus strictes du continent européen.

Quatrièmement, le modèle suisse bénéficie d'une crédibilité internationale, grâce à la conformité de la législation aux normes du GAFI, à la participation au Groupe Egmont et à la mise en œuvre de la norme CRS de l'OCDE. La Suisse est ainsi considérée comme fiable au niveau international, ce qui explique pourquoi elle ne figure plus sur aucune liste grise du GAFI depuis 2019.

Een vijfde sterkte is het evenwicht tussen privacy en transparantie. De kracht van het Zwitsers model schuilt in dat juridisch evenwicht, wat in België dus zoek zal zijn door de voorliggende hervorming. Alles zal gebeuren in functie van de efficiëntie en ten koste van de privacy.

Dat evenwicht is er dus wel in Zwitserland. De overheid beschikt er over de noodzakelijke instrumenten waar de burgers behouden een reëel gevoel van financiële privacy. Dat vertrouwen draagt bij aan de stabiliteit van het bankwezen en de bereidheid van instellingen om vrijwillig te rapporteren.

Er blijven tegelijk zwaktes en structurele uitdagingen aan het Zwitserse systeem. In de eerste plaats is er de federale versnippering. De verdeling van de bevoegdheden tussen 26 kantons leidt soms tot inconsistenties. Niet alle kantonale parketten gebruiken hetzelfde rapportageformaat of dezelfde technische interface met MROS. Dit bemoeilijkt statistische uniformiteit en kan het onderzoek vertragen.

Er zijn ook de beperkte zoekmogelijkheden. Omdat alleen MROS zoekopdrachten mag uitvoeren, klagen justitieautoriteiten over wachttijden in urgente dossiers. Een voorstel voor een beperkte rechtstreekse toegang met een ex-postcontrole ligt op tafel maar stuit op weerstand van privacywaakhonden.

Ten derde wordt door sommigen het gebrek aan *data-mining* als een zwakte voorzien. De spreker zelf vindt het eerder een sterkte. Het verbod op grootschalige patroonherkenning voorkomt misbruik, maar beperkt ook de preventieve capaciteit. Dat staat in schril contrast met wat men van plan is in België te doen.

De fractie van de spreker wil met deze tussenkomst de burger informeren over die plannen. Het licht toe waarom de fractie zich verzet tegen de massale surveillance, privacy-intrusie, het schenden van het privéleven en vooral het schenden van het vermoeden van onschuld.

De heer Van Quickenborne wijst voorts op de politieke weerstand. Elke poging in Zwitserland om de bevoegdheden van MROS uit te breiden, stuit op terughoudendheid in het parlement. Liberale partijen in Zwitserland zien elke uitbreiding als een stap in de richting van de afschaffing van het bankgeheim. Open Vld herkent zich in die houding.

Men moet ook vaststellen dat de internationale druk groot is. De toekomstige *Authority for Anti-Money Laundering* van de EU zal een uniform gegevensraamwerk

La force du modèle suisse réside en outre dans un cinquième atout, à savoir l'équilibre juridique entre vie privée et transparence, qui disparaîtra en Belgique si la réforme à l'examen est adoptée. La part belle sera faite à l'efficacité, au détriment de la vie privée.

En Suisse, cet équilibre existe bel et bien. L'État y dispose des instruments nécessaires, tandis que les citoyens conservent un véritable sentiment de vie privée financière. Cette confiance contribue à la stabilité du secteur bancaire et à la disposition des établissements à faire des signalements volontaires.

Dans le même temps, plusieurs faiblesses et défis structurels subsistent dans le système suisse. En premier lieu, il y a la fragmentation fédérale. La répartition des compétences entre 26 cantons entraîne parfois des incohérences. Tous les parquets cantonaux n'utilisent pas le même format de communication ni la même interface technique dans leurs contacts avec le MROS. Cette situation complique l'uniformité statistique et peut ralentir les enquêtes.

En outre, les possibilités de recherche sont limitées. Comme seul le MROS peut effectuer des recherches, les autorités judiciaires se plaignent de délais d'attente dans les dossiers urgents. Une proposition visant à instaurer un accès direct limité avec un contrôle *ex post* est à l'examen, mais elle se heurte à l'opposition des défenseurs de la vie privée.

Troisièmement, certains considèrent l'absence d'exploration de données comme une faiblesse. L'intervenant y voit plutôt une force. L'interdiction de la reconnaissance de modèles à grande échelle empêche les abus, mais limite aussi la capacité préventive. Le contraste avec les textes à l'examen en Belgique est important.

Le groupe de l'intervenant entend, par cet exposé, informer le citoyen des projets en cours. L'intervenant souhaite expliquer pourquoi son groupe s'oppose à la surveillance de masse, aux intrusions dans la sphère privée, aux violations de la vie privée et surtout à la violation de la présomption d'innocence.

M. Van Quickenborne met en outre l'accent sur la résistance politique. En Suisse, toute tentative d'élargir les attributions du MROS se heurte aux réticences du Parlement. Les partis libéraux helvètes considèrent toute extension de ces attributions comme un pas vers la suppression du secret bancaire. L'Open Vld est du même avis.

Force est aussi de constater que la pression internationale est forte. La future Autorité de lutte contre le blanchiment de capitaux de l'UE imposera un cadre de

opleggen. Zwitserland, alhoewel geen EU-lidstaat, zal zich moeten aanpassen om een gelijkwaardige samenwerking te behouden. Dat kan leiden tot de verdere openstelling van rekeninginformatie, wat politiek gevoelig is en blijft.

Verder toont de spreker aandacht voor de evaluatie in de context van financiële integriteit, met vooreerst de impact op de witwasbestrijding. De FATF kende in een evaluatie van 2022 Zwitserland de score van “substantieel effectief” toe op de meeste criteria. Het land scoort hoog op meldingsdiscipline, maar lager op snelheid van informatie-uitwisseling. De eerder gemelde duurtijd van 6 uur lijkt inderdaad aan de trage kant. Toch behoort Zwitserland tot een van de meeste efficiënte CFI's.

Er is tevens de impact of het effect op het bankwezen. De aanwezigheid van een goed functionerend aanspreekpunt verhoogt het vertrouwen van internationale cliënten en tegenpartijen. Banken kunnen aantonen dat zij actief bijdragen aan de integriteitsbewaking zonder vertrouwelijke klantinformatie publiek te maken. Dit is de rol in internationale samenwerking. Dankzij de duale structuur – MROS voor witwaszaken en ESTV voor fiscale uitwisseling – kan Zwitserland flexibel inspelen op bilaterale en multilaterale verzoeken. Het land fungeert als brug tussen de EU-landen en jurisdicties met strengere privacywetten zoals Singapore en Hongkong.

Als tussentijdse conclusie kan worden gesteld dat de evaluatie aantoont dat het Zwitserse Kontenregister een evenwichtige en robuuste infrastructuur is. Het is juist dat het minder open is dan EU-registers, maar daardoor ook stabiel in de rechtsstatelijke zin. De belangrijkste sterkte ligt in de betrouwbaarheid en de precisie van de data, en de voornaamste uitdaging in de nood aan snellere toegang en technologische integratie.

De heer Van Quickenborne besteedt vervolgens aandacht aan de beleidsaanbevelingen, de hervormingsrichtingen en de conclusies. De strategische uitgangspunten voor een hervorming hebben een dubbel beleidsdoel. De Zwitserse Bondsraad hanteert sinds 2023 twee complementaire uitgangspunten: (1) het behoud van vertrouwen en financiële privacy als concurrentievoordeel van de Zwitserse financiële sector en (2) de volledige naleving van internationale normen inzake anti-witwassen maar evenzeer inzake anti-terrorismedinanciering.

données uniforme. La Suisse, bien qu'elle ne soit pas membre de l'UE, devra s'adapter afin de maintenir une coopération équivalente. En conséquence, elle pourrait devoir assurer une transparence accrue des informations relatives aux comptes bancaires, ce qui est et restera politiquement sensible.

Puis, l'intervenant évoque la question de l'évaluation dans le cadre de l'intégrité financière, et d'abord son incidence sur la lutte contre le blanchiment. Dans une évaluation réalisée en 2022, le GAFI a attribué à la Suisse la notation “niveau d'efficacité significatif” pour la plupart des critères évalués. Ce pays obtient un score élevé pour sa discipline en matière de notification, mais un score moins élevé pour sa rapidité à échanger des informations. Le délai de 6 heures précité semble en effet un peu long. Néanmoins, la Suisse possède l'une des CTIF les plus efficaces.

Il convient aussi d'évoquer l'incidence ou l'effet du point de contact sur le secteur bancaire. La présence d'un point de contact de qualité renforce la confiance des clients et des contreparties internationaux. Les banques peuvent démontrer qu'elles contribuent activement au contrôle de l'intégrité sans divulguer d'informations confidentielles sur leurs clients. Tel est leur rôle dans la coopération internationale. Grâce à sa structure duale – MROS pour les affaires de blanchiment et ESTV pour l'échange d'informations fiscales – la Suisse peut répondre de manière flexible aux demandes bilatérales et multilatérales. Le pays sert d'intermédiaire entre les pays de l'Union européenne et les juridictions appliquant des législations plus strictes en matière de respect de la vie privée, comme Singapour et Hong Kong.

À titre de conclusion intermédiaire, on peut affirmer que l'évaluation démontre que le registre suisse des comptes est une infrastructure équilibrée et robuste. Il est exact que ce registre est moins ouvert que les registres européens, mais cela le rend aussi plus stable sur le plan du respect de l'état de droit. Sa principale force réside dans la fiabilité et la précision de ses données, et son principal défi dans la nécessité de permettre un accès plus rapide et une intégration technologique.

M. Van Quickenborne évoque ensuite les recommandations stratégiques, les pistes de réforme et les conclusions. Les principes stratégiques d'une réforme poursuivent un double objectif politique. Depuis 2023, le Conseil fédéral suisse applique deux principes complémentaires: (1) la sauvegarde de la confiance et de la vie privée financière comme avantage concurrentiel du secteur financier suisse et (2) le respect total des normes internationales en matière de lutte contre le blanchiment, mais aussi contre le financement du terrorisme.

De hervorming van de GwG is bedoeld om deze doelen te verzoenen. Het is geen breuk met het verleden. Het is een modernisering van het evenwicht dat sinds de jaren 1990 bestaat tussen geheimhouding en transparantie.

Het bankgeheim is een van de pijlers van het functioneren van de Zwitserse Staat, en werd vastgelegd in artikel 47 van de bankwet van 1933. Dat blijft juridisch van kracht, maar de interpretatie ervan is geëvolueerd. Vandaag beschermt het bankgeheim de burger tegen onrechtmatige inzagen, maar niet de fraudeur tegen rechtmatige opsporing. Dat onderscheid vormt de kern van het Zwitserse model 2.0. Het Kontenregister concretiseert dit principe: informatie is afgeschermd maar traceerbaar voor wie wettelijk bevoegd is. Er is politieke consensus, want ondanks de ideologische verschillen bestaat in de Bondsraad een groeiende consensus dat Zwitserland geen geïsoleerde enclave kan blijven. Zelfs de liberale FDP herkent de noodzaak van harmonisatie met de Europese standaard. De linkse fracties pleiten voor meer transparantie, terwijl de SVP, die andere conservatieve partij, vooral waarborgen eist tegen misbruik. De hervormingsagenda wordt dus breed gedragen, maar moet zorgvuldig worden uitgevoerd om het delicate evenwicht te bewaren.

Wat betreft de voorgestelde hervormingsrichtingen gelden de volgende opmerkingen. De huidige wetgeving bevat geen expliciete bepaling die het Kontenregister als zodanig benoemt. Er zal evenwel worden voorzien in een bepaling die de juridische status van het register versterkt en die rechtszekerheid creëert voor rechtsinstellingen en onderzoekers.

Verder zal aan de hand van een voorgestelde hervormingsrichting gezorgd voor de snellere toegang voor rechtelijke autoriteiten. Momenteel kunnen de politie en de parketten enkel informatie opvragen via MROS. Er wordt daarom voorgesteld om een fast-track-procedure in te voeren voor urgente gevallen, en dat mits bepaalde waarborgen. Zo wordt snelheid gecombineerd met verantwoordingsplicht.

Er wordt tevens gezorgd voor de uniformering van de kantonale procedures. De Bondsraad stelt een federale interoperabiliteitsnorm voor die alle kantonale parketten verplicht het goAML-protocol te gebruiken. Dit voorkomt dubbel werk en versnelt de gegevensuitwisseling. Een federaal steunfonds zou de technologische upgrade van kleinere kantons kunnen financieren.

Er komt ook een integratie met het UBO-register. Zwitserland bereidt de invoering voor van een register

La réforme de la LBA vise à concilier ces objectifs. Il ne s'agit pas d'une rupture avec le passé, mais d'une modernisation de l'équilibre qui existe depuis les années 1990 entre secret et transparence.

Le secret bancaire est l'un des piliers du fonctionnement de l'État suisse, et a été inscrit dans l'article 47 de la loi suisse sur les banques de 1933. Cet article reste en vigueur sur le plan juridique, mais son interprétation a évolué. Aujourd'hui, le secret bancaire protège le citoyen contre les consultations illégales, mais pas le fraudeur contre les enquêtes légitimes. Cette distinction est au cœur du modèle suisse 2.0. Le registre suisse des comptes concrétise ce principe: les informations sont protégées mais traçables pour ceux qui sont légalement habilités à le faire. Il existe un consensus politique, car, malgré les divergences idéologiques en son sein, le Conseil fédéral s'accorde de plus en plus à reconnaître que la Suisse ne peut rester une enclave isolée. Même le Parti libéral-radical suisse (PLR) reconnaît la nécessité d'une harmonisation avec les normes européennes. Les groupes de gauche préconisent une plus grande transparence, tandis que l'UDC, l'autre parti conservateur, exige avant tout des garanties contre les abus. Le programme de réforme est donc largement soutenu, mais doit être mis en œuvre avec prudence en vue de préserver l'équilibre fragile qui existe.

En ce qui concerne les pistes de réforme proposées, l'intervenant formule les observations suivantes. La législation actuelle ne contient aucune disposition explicite mentionnant le registre des comptes en tant que tel. Toutefois, une disposition renforçant le statut juridique de ce registre et créant de la sécurité juridique pour les institutions judiciaires et les enquêteurs sera prévue.

En outre, une proposition de piste de réforme vise à permettre aux autorités judiciaires d'accéder plus rapidement au registre. Actuellement, la police et les parquets ne peuvent demander des informations que par l'intermédiaire du MROS. Il est donc proposé d'instaurer une procédure accélérée pour les cas urgents, sous réserve de certaines garanties. La célérité sera ainsi conjuguée au principe de responsabilité.

L'uniformisation des procédures cantonales sera également assurée. Le Conseil fédéral suisse propose une norme fédérale d'interopérabilité imposant à tous les parquets cantonaux d'utiliser le protocole goAML. Cette procédure évitera les doublons et accélérera l'échange de données. Un fonds fédéral de soutien pourrait financer la mise à niveau technologique des cantons de plus petite taille.

Une intégration avec le registre UBO est également prévue. La Suisse prépare la mise en place d'un registre

van Ultimate Beneficial Owners. De koppeling tussen UBO-gegevens en het Kontenregister is cruciaal om complexe eigendomsrechten te doorgronden. Het plan voorziet een *privacy preserving linkage* waarbij enkel geautoriseerde onderzoekers de relatie kunnen zien tussen rekeningen en achterliggende personen. De gegevens worden technisch gekoppeld via cryptografische pseudoniemen en niet via naamidentificatie.

Inzake de toekomstige toepassing van kunstmatige intelligentie geldt de vaststelling dat, in tegenstelling tot *datamining*, Zwitserland AI wil gebruiken over de volledige dataset doch binnen strikt omschreven dossiers. De *Digital Finance Integrity Strategy* voorziet experimenten met *machine learning* voor anomaliedetectie in de workflow van MROS zonder dat deze algoritmen buiten het onderzoeksdossier om zoeken. EDÖB en FINMA zullen toezicht houden via verplichte *algorithmic impact assessments*.

De spreker komt vervolgens tot de economische en institutionele effecten. De Zwitserse bankenvereniging berekende dat de hervorming jaarlijks ongeveer 45 miljoen Zwitserse frank extra compliance kosten met zich zal meebrengen, maar ook voor ongeveer 30 % tijdswinst zal zorgen bij rechtshulpverzoeken. De sector ziet dit als een investering in zijn reputatie. Transparantie versterkt immers de internationale geloofwaardigheid.

Na de impact op de bankensector wil de spreker de blik werpen op de institutionele samenwerking. De hervorming stimuleert een nauwere samenwerking tussen MROS (de operationele hub), FINMA (de toezichthouder op de instellingen), ESTV (de fiscale coördinator) en EDÖB (de toezichthouder op de privacy). Deze vier instellingen moeten beter met mekaar gaan samenwerken. Zij vormen samen het quadriga-model van de Zwitserse financiële integriteit. Het model garandeert dat geen enkele instantie de alleenheerschappij heeft over data, wat machtsconcentratie voorkomt.

De federale regering van Zwitserland, in gesprekken met de Europese Commissie, zegt toe het Zwitserse systeem tegen 2027 aan te sluiten op het *EU bank account registers interconnection system* (BARIS), mits de volledige datasoevereiniteit behouden blijft.

des bénéficiaires effectifs. La connexion entre les données UBO et le registre suisse des comptes sera cruciale pour comprendre les droits de propriété complexes. Le projet prévoit une connexion préservant la vie privée (*privacy preserving linkage*) qui permettra uniquement aux enquêteurs habilités à prendre connaissance du lien entre les comptes et leurs détenteurs. Sur le plan technique, les données seront couplées via la pseudonymisation cryptographique, et pas via l'identification par nom.

En ce qui concerne l'application future de l'intelligence artificielle, force est de constater que, contrairement à l'exploration de données, la Suisse souhaite utiliser l'IA sur l'ensemble des données mais dans le cadre de dossiers strictement définis. La stratégie numérique d'intégrité financière prévoit des expériences d'apprentissage automatique (*machine learning*) visant à détecter des anomalies dans le flux de travail du MROS, sans que ces algorithmes ne procèdent à des recherches en dehors du dossier d'enquête. Le PFPDT et la FINMA exerceront une surveillance au moyen d'évaluations obligatoires d'impact algorithmique.

L'intervenant aborde ensuite les répercussions économiques et institutionnelles. L'Association suisse des banquiers a calculé que les coûts de mise en conformité s'élèveraient à quelque 45 millions de francs suisses par an, mais que cette réforme permettrait également un gain de temps d'environ 30 % dans le traitement des demandes d'entraide judiciaire. Le secteur considère cette réforme comme un moyen d'investir dans sa réputation. La transparence renforce en effet la crédibilité internationale.

Après avoir examiné les retombées sur le secteur bancaire, l'intervenant souhaite se pencher sur la collaboration institutionnelle. La réforme encourage une collaboration plus étroite entre le MROS (le point de contact central), la FINMA (l'autorité de surveillance du marché financier), l'AFC (le coordinateur fiscal) et le PFPDT (l'autorité de protection des données). Ces quatre institutions, qui forment ensemble le modèle quadripartite de l'intégrité financière suisse, doivent apprendre à mieux collaborer entre elles. Ce modèle garantit qu'aucune instance n'a le monopole absolu des données, ce qui empêche toute concentration du pouvoir.

Le gouvernement fédéral suisse, dans ses discussions avec la Commission européenne, s'engage à relier le système suisse au Système d'interconnexion des registres des comptes bancaires de l'UE (BARIS) d'ici 2027, sous réserve du maintien intégral de la souveraineté en matière de données.

Wat de beleidscoördinatie betreft, stelt de federale regering van Zwitserland voor een coördinatieraad voor financiële integriteit op te richten. Deze raad rapporteert jaarlijks over de implementatie van het Kontenregister en formuleert aanbevelingen aan het Zwitserse parlement. Daarnaast publiceert de coördinatieraad een openbaar jaarverslag met statistieken, geanonimiseerde casussen en beveiligingsincidenten. Die transparantie vormt een noodzakelijk tegenwicht voor het niet-publieke karakter van het register. De federale regering van Zwitserland overweegt om elke vijf jaar een onafhankelijke evaluatie te laten uitvoeren door academische instellingen. Zulke evaluaties moeten beleidsneutraliteit verzekeren en technologische trends tijdig signaleren.

Vervolgens plaatst de heer Van Quickenborne dit alles in een breder Europees en mondiaal perspectief. Zwitserland neemt volgens hem een unieke positie in en fungeert als brug tussen transparantie en vertrouwelijkheid. Landen met een vergelijkbare traditie, zoals Liechtenstein en Monaco, volgen het Zwitserse model bij de hervorming van hun witwasbeleid.

De *Financial Action Task Force*, oftewel de FATF-ronde, van 2026 zal bijzondere aandacht besteden aan digitalisering en internationale samenwerking. Zwitserland bereidt zich hierop voor door uitbreiding van realtime informatie-uitwisseling, invoering van een uniform identificatiesysteem voor rekeningen (het UBIN-systeem) en standaardisering van metadata volgens FATF-aanbeveling 29*bis*. Deze maatregelen versterken de compatibiliteit met Europese en OESO-datastandaarden.

Het lid vergelijkt vervolgens de positie van de EU met die van Zwitserland. Waar de EU werkt met AMLA en BARIS, supranationaal en bindend voor de lidstaten, hanteert Zwitserland een nationaal systeem, IMROS. Uitwisseling met de EU gebeurt via BARIS, terwijl Zwitserland bilateraal samenwerkt. Terwijl de EU de GDPR en de EU Data Act toepast, beschikt Zwitserland over de DSG en staat de EDUB in voor toezicht. De beleidsoпvolgning verloopt in de EU via de bestuursraad van AMLA, terwijl Zwitserland daarvoor de coördinatieraad voor financiële integriteit aanwijst. Technologisch gebruikt de EU de BARIS API, terwijl Zwitserland werkt met GoML en de Swiss GovCloud. Zo blijft Zwitserland compatibel, maar bewaart het tegelijk zijn beleidssovereiniteit.

En ce qui concerne la coordination des politiques, le gouvernement fédéral suisse propose de créer un conseil de coordination pour l'intégrité financière. Ce conseil rendra chaque année un rapport sur la mise en œuvre du Registre des comptes et formulera des recommandations au Parlement suisse. En outre, le conseil de coordination publiera un rapport annuel public comportant des statistiques, des cas d'espèce anonymisés et des incidents de sécurité. Cette transparence constitue un contrepoids nécessaire au caractère non public du registre. Le gouvernement fédéral suisse envisage de faire réaliser tous les cinq ans une évaluation indépendante par des institutions académiques. De telles évaluations devront permettre de garantir la neutralité des politiques et de signaler en temps utile les tendances technologiques.

M. Van Quickenborne replace ensuite ces divers éléments dans une perspective européenne et mondiale plus large. Selon lui, la Suisse occupe une position unique et fait le lien entre transparence et confidentialité. Des pays ayant une tradition comparable, tels que le Liechtenstein et Monaco, suivent le modèle suisse dans la réforme de leur politique de lutte contre le blanchiment d'argent.

Le Groupe d'action financière (GAFI), lors de son cycle de 2026, accordera une attention particulière à la numérisation et à la coopération internationale. La Suisse s'y prépare par l'extension des échanges d'informations en temps réel, l'introduction d'un système uniforme d'identification des comptes (système UBIN) et la standardisation des métadonnées conformément à la recommandation 29*bis* du GAFI. Ces mesures renforcent la compatibilité avec les standards de données européens et de l'OCDE.

Le membre compare ensuite la position de l'Union européenne à celle de la Suisse. Alors que l'Union européenne s'appuie sur l'AMLA et sur le système d'interconnexion des RCB (BARIS), une autorité et un système supranationaux contraignants pour les États membres, la Suisse applique un système national, le MROS. Les échanges avec l'Union européenne ont lieu au travers du système d'interconnexion des RCB, tandis que la Suisse noue des collaborations bilatérales. Alors que l'Union européenne applique le RGPD et le Règlement UE sur la protection des données, la Suisse dispose de la DSG (loi sur la protection des données) et confie les contrôles au PFPDT. Le suivi politique s'effectue, dans l'Union européenne, par le conseil d'administration de l'AMLA, tandis que la Suisse désigne à cet effet le conseil de coordination pour l'intégrité financière. Sur le plan technologique, l'Union européenne utilise le BARIS API, tandis que la Suisse recourt à GoML et au Swiss GovCloud. Ainsi, la Suisse reste compatible avec l'Union européenne tout en préservant sa souveraineté politique.

Vervolgens overloopt de heer Van Quickenborne acht beleidsaanbevelingen.

Er wordt ten eerste gepleit voor wettelijke verankering van het Kontenregister met duidelijke bevoegdheidsafbakening. Ten tweede zal de toegangsmethodiek worden hervormd met snelle elektronische verzoeken in spoedgevallen, maar steeds met logging en ex-postcontrole. De derde aanbeveling omvat de integratie van UBO-gegevens via privacyvriendelijke koppelingen. De vierde aanbeveling is de uniformering van kantonale procedures en financiering van technologische aanpassingen. De volgende, vijfde, aanbeveling betreft de versterking van de rol van de EDUB bij het toezicht op algoritmen en datakoppelingen. Een zesde punt omvat de stimulering van innovatie via investeringen in AI-ondersteunde anomaliedetectie binnen duidelijke ethische kaders. De zevende aanbeveling behelst publicatie van jaarlijkse geaggregeerde statistieken ter versterking van de publieke legitimiteit. De achtste en laatste aanbeveling is de ontwikkeling van een diplomatieke strategie om samenwerking met de EU en de FATF te institutionaliseren.

In zijn conclusie benadrukt de heer Van Quickenborne dat het Zwitserse Kontenregister de evolutie weerspiegelt van absoluut bankgeheim naar gereguleerde transparantie. Waar voorheen discretie centraal stond, staat nu gerichte toegankelijkheid voorop. Volgens hem bewijst het IMROS-systeem dat integriteit en privacy niet tegenover elkaar hoeven te staan, maar elkaar kunnen versterken wanneer ze juridisch stevig zijn verankerd.

Uit de analyse blijkt dat Zwitserland een robuust en doeltreffend model heeft opgezet dat internationaal wordt gewaardeerd en dat zowel de witwasbestrijding als de stabiliteit van de financiële sector en het vertrouwen van de burgers versterkt. De uitdaging voor het volgende decennium bestaat erin dit evenwicht te handhaven in een context van toenemende digitalisering en grensoverschrijdende informatiestromen. Met de aangekondigde hervormingen en de oprichting van de coördinatieraad voor financiële integriteit acht de heer Van Quickenborne dat Zwitserland goed gepositioneerd is om deze uitdaging aan te gaan als moderne, betrouwbare en transparante financiële natie.

De heer Van Quickenborne besluit dat landenoverzicht nu is afgerond en vervolgt met een korte schets van de inhoudstafel van zijn pleidooi.

In hoofdstuk 1 heeft hij reeds gewezen op de noodzaak van een breed maatschappelijk debat.

M. Van Quickenborne passe ensuite en revue huit recommandations politiques.

Une première recommandation préconise l'ancrage légal du Registre des comptes avec une délimitation claire des compétences. Deuxièmement, il convient de réformer la méthodologie d'accès au travers de demandes électroniques rapides en cas d'urgence, mais toujours assorties d'un logging et d'un contrôle *ex post*. La troisième recommandation prévoit l'intégration des données UBO au moyen de connexions respectueuses de la vie privée. La quatrième recommandation porte sur l'uniformisation des procédures cantonales et le financement des adaptations technologiques. Cinquièmement, il y a lieu de renforcer le rôle du PFPDT dans le contrôle des algorithmes et des connexions de données. Sixièmement, il faut stimuler l'innovation par des investissements dans la détection d'anomalies assistée par l'IA, en prévoyant des cadres éthiques clairs. La septième recommandation porte sur la publication de statistiques agrégées annuelles afin de renforcer la légitimité publique. La huitième et dernière recommandation a trait au développement d'une stratégie diplomatique pour institutionnaliser la coopération avec l'Union européenne et le GAFI.

En conclusion, M. Van Quickenborne souligne que le Registre des comptes suisse reflète l'évolution du secret bancaire absolu vers une transparence régulée. Là où la discrétion était autrefois centrale, l'accessibilité ciblée est désormais prioritaire. Selon lui, le système MROS démontre que l'intégrité et le respect de la vie privée ne doivent pas s'opposer, mais peuvent se renforcer mutuellement lorsqu'ils sont solidement ancrés au niveau juridique.

Il ressort de l'analyse que la Suisse a mis en place un modèle robuste et efficace, apprécié au niveau international, qui renforce à la fois la lutte contre le blanchiment, la stabilité du secteur financier et la confiance des citoyens. Le défi de la prochaine décennie consiste à maintenir cet équilibre dans un contexte de numérisation croissante et de flux d'informations transfrontaliers. Avec les réformes annoncées et la création du conseil de coordination pour l'intégrité financière, M. Van Quickenborne estime que la Suisse est bien positionnée pour relever ce défi en tant que nation financière moderne, fiable et transparente.

M. Van Quickenborne conclut que l'aperçu par pays est désormais terminé et poursuit par un bref résumé de la table des matières de son plaidoyer.

Dans le chapitre 1^{er}, il a déjà souligné la nécessité d'un large débat sociétal.

Het commissielid benadrukt dat het centrale thema van de bespreking, *money control*, bijzonder belangrijk is. Hij verwijst naar het voornemen van de overheid om toegang te krijgen tot de bankrekeningen van alle elf miljoen Belgen. Het doel van dit debat bestaat erin de burger wakker te schudden en een effect te creëren zoals in het Europees Parlement, waar burgers uiteindelijk het voorstel rond *chat control* hebben afgewezen. Dat systeem beoogde alle berichten van burgers te screenen op mogelijk beeldmateriaal van kindermisbruik. Volgens het lid doet zich hier een identieke problematiek voor waarbij de proportionaliteit zoek is. Terwijl Parlement en meerderheid zwijgen, roert de straat zich en groeit het aantal Belgische burgers dat zich vragen stelt.

In het tweede hoofdstuk ging het lid in op de stilte in de pers. Deze laatste besteedt steeds meer aandacht aan de kwestie. Volgens hem is dat precies de bedoeling van het debat: de voor- en nadelen zorgvuldig tegen elkaar afwegen. De Open Vld is uiteraard voor fraudebestrijding is, maar deze moet proportioneel blijven. Het is namelijk volstrekt disproportioneel om fraude te bestrijden door alle bankrekeningen van alle Belgen systematisch te controleren, inclusief die van burgers die in geen enkel opzicht met fraude in verband kunnen worden gebracht. Volgens hem schendt het voorstel *money control* manifest het privéleven van burgers.

De heer Van Quickenborne richt zich vervolgens tot de minister en stelt dat deze de oplossing in handen heeft: hij kan het voorliggende wetsontwerp intrekken uit de parlementaire behandeling. Zolang er geen afdoende antwoorden worden gegeven en vooral zolang privacy en het vermoeden van onschuld niet worden gegarandeerd, blijft het verzet van de Open Vld onverzettelijk.

In hoofdstuk 3 werden de gelijkenissen tussen *chat control* 1.0 en 2.0 besproken. Het lid verwees hierbij naar het recent werk van Kjell Van der Elst (Open Vld), die aantoonde dat men in het Europees Parlement langs een achterpoortje alsnog probeert *chat control* 2.0 door te voeren, wat volgens hem problematisch is.

Verder bespreekt het lid de ontbrekende adviezen. De Raad van State wijst immers op het ontbreken van essentiële adviezen van de Nationale Bank, de Europese Centrale Bank en de Inspecteur van Financiën. Zolang deze adviezen niet beschikbaar zijn, kunnen de parlementsleden volgens de heer Van Quickenborne geen gefundeerd oordeel vormen.

In hoofdstuk 5 behandelde het commissielid de geschiedenis van het CAP, dat sinds 2011 bestaat en is ingevoerd om te voldoen aan een Europese verplichting.

Le membre insiste sur le fait que le thème central de la discussion, le *money control*, est particulièrement important. Il renvoie à l'intention des pouvoirs publics d'accéder aux comptes bancaires des onze millions de Belges. L'objectif du présent débat est de réveiller les citoyens, comme cela a été le cas concernant la proposition du Parlement européen relative au *chat control*, qu'ils ont finalement rejetée. Ce système visait à examiner tous les messages des citoyens afin d'y détecter d'éventuelles images d'abus d'enfants. Selon le membre, une problématique identique se présente en l'espèce: le principe de proportionnalité n'est pas respecté. Alors que le Parlement et la majorité gardent le silence, la rue s'agite et un nombre croissant de citoyens belges se posent des questions.

Dans le chapitre 2, le membre a abordé l'attitude de la presse. D'abord silencieuse, elle consacre de plus en plus d'attention à la question. Selon lui, c'est précisément le but du présent débat: mettre soigneusement en balance les avantages et les inconvénients. L'Open Vld est évidemment favorable à la lutte contre la fraude, mais celle-ci doit rester proportionnée. Il est en effet totalement disproportionné de combattre la fraude en contrôlant systématiquement tous les comptes bancaires de l'ensemble des Belges, y compris ceux qui ne peuvent en aucune manière être liés à une fraude. Selon lui, la proposition *money control* viole manifestement la vie privée des citoyens.

M. Van Quickenborne s'adresse ensuite au ministre et affirme que celui-ci a la solution en main: il peut retirer le projet de loi à l'examen du circuit parlementaire. Tant que des réponses adéquates ne seront pas apportées et, surtout, tant que la vie privée et la présomption d'innocence ne seront pas garanties, l'Open Vld continuera de s'y opposer fermement.

Au chapitre 3, les similitudes entre le *chat control* 1.0 et 2.0 ont été examinées. Le membre a renvoyé à une étude récente de Kjell Van der Elst (Open Vld), qui a démontré que le Parlement européen tente d'instaurer en catimini un *chat control* 2.0, ce qui pose problème selon lui.

Le membre évoque ensuite les avis manquants. Le Conseil d'État relève en effet l'absence d'avis essentiels de la BNB, de la Banque centrale européenne et de l'Inspecteur des Finances. Selon M. Van Quickenborne, tant que ces avis ne seront pas disponibles, les parlementaires ne pourront pas se forger un jugement éclairé.

Au chapitre 5, le membre a parlé de l'historique du PCC, qui existe depuis 2011 et a été instauré pour répondre à une obligation européenne. L'actuel PCC

Het huidige CAP laat de fiscus toe om, in gevallen van vermoeden van belastingontduiking waarbij de betrokkene niet wil meewerken, te achterhalen waar iemand bankrekeningen aanhoudt. De Open Vld staat achter dat systeem, dat bovendien door het Grondwettelijk Hof is getoetst.

Het lid onderstreept echter dat het huidige voorliggende wetsontwerp van de arizonaregering een ware paradigmaverschuiving inhoudt: niet langer controleert men enkel personen die verdacht worden van fraude, voortaan zou men iedereen controleren, in de hoop enkele fraudeurs te vinden.

In hoofdstuk 6 werd het toetsingskader en de nationale privacywetgeving besproken samen met de rol van de Gegevensbeschermingsautoriteit (GBA) en haar adviezen. Bij de uitwerking van het CAP in 2011 en 2018 heeft ook de toenmalige commissie voor de Privacy, de voorloper van de GBA, advies uitgebracht. Dat advies bevatte elf kritische punten. Uiteindelijk hield de wet van 2018 rekening met die opmerkingen en bovendien is die wet tot op heden nooit door een rechtbank vernietigd.

De spreker behandelt in hetzelfde kader artikel 22 van de Grondwet, het recht op privacy en artikel 22*bis*, dat het recht op privacy voor kinderen verankert. Hij benadrukt dat de opname van een specifiek grondwetsartikel voor de privacy van kinderen aangeeft hoe groot de belangen zijn en hoezeer hun privacy moet worden beschermd. Het commissielid wijst erop dat het wetsontwerp van de minister erin voorziet dat zelfs bankrekeningen van minderjarigen aan datamining worden onderworpen. Hoe kan een kind van zes of negen jaar ooit verdacht worden van fraude? Analyse van rekeningen van personen met zeer grote vermogens is volgens hem bespreekbaar, maar niet van burgers met beperkte middelen.

Ten slotte verwijst hij naar de rechtspraak van het Europees Hof voor de Rechten van de Mens en het Hof van Justitie, die strenge proportionaliteitseisen stellen aan dataretentie. De recente, op die rechtspraak afgestemde dataretentiewet houdt vooralsnog stand.

In hoofdstuk 7 maakte het lid een internationale vergelijking tussen acht landen, waarvan zeven Europese lidstaten, die volgens hem duidelijk de weg vooruit tonen en zich resoluut verzetten tegen datamining en *money control*.

In hoofdstuk 8 besprak de heer Van Quickenborne de Europese dataruimte. Vervolgens werd gefocust op

permet au fisc, lorsqu'il existe un soupçon de fraude fiscale et que la personne concernée refuse de coopérer, de déterminer auprès de quel(s) établissement(s) celle-ci détient des comptes bancaires. L'Open Vld soutient ce système, qui a d'ailleurs été examiné par la Cour constitutionnelle.

Le membre souligne toutefois que le projet de loi à l'examen du gouvernement Arizona vise à opérer un véritable changement de paradigme: il ne s'agirait plus de contrôler uniquement les personnes soupçonnées de fraude, mais de contrôler désormais tout un chacun, dans l'espoir de repérer quelques fraudeurs.

Au chapitre 6, le cadre d'évaluation et la législation nationale concernant la protection de la vie privée ont été abordés, de même que le rôle de l'Autorité de protection des données (APD) et de ses avis. Lors de l'élaboration du PCC en 2011 et en 2018, la Commission Vie privée, ancêtre de l'APD, avait également rendu un avis. Cet avis comportait onze points critiques. En définitive, la loi de 2018 a tenu compte de ces observations et, au demeurant, cette loi n'a jamais été annulée par une juridiction à ce jour.

L'intervenant aborde dans le même contexte l'article 22 de la Constitution, qui traite du droit au respect de la vie privée, et l'article 22*bis*, qui consacre le droit au respect de la vie privée des enfants. Le membre souligne que le fait qu'un article spécifique consacré à la vie privée des enfants figure dans la Constitution montre à quel point les intérêts en présence sont fondamentaux et à quel point il est important de protéger la vie privée des enfants. Le membre signale que le projet de loi du ministre prévoit que même les comptes bancaires des mineurs seront soumis au *data mining*. Comment un enfant de six ou neuf ans pourrait-il être suspecté de fraude? On peut éventuellement envisager d'analyser les comptes de personnes très fortunées, mais pas ceux de citoyens disposant de moyens limités.

Enfin, il renvoie à la jurisprudence de la Cour européenne des droits de l'homme et de la Cour de justice, qui impose des exigences strictes de proportionnalité en matière de rétention des données. La récente loi sur la rétention des données, qui est alignée sur cette jurisprudence, reste en vigueur à ce stade.

Dans le chapitre 7, le membre a établi un parallèle international entre huit pays, dont sept États membres de l'Union européenne, qui, selon lui, montrent clairement la voie à suivre et s'opposent résolument au *data mining* et au *money control*.

Dans le chapitre 8, M. Van Quickenborne a évoqué la question de l'Espace européen de données. Il s'est

enkele bijkomende bepalingen in de wettekst, waaronder de toevoeging van crypto-activa en de opname van effectenrekeningen in het CAP. Hij plaatste daarbij een aantal kritische kanttekeningen om vervolgens over te gaan tot bespreking van de zeven alinea's, opgenomen in amendementen van de regering, die de contouren van *money control* bepalen.

Het commissielid verwijst voorts opnieuw naar het kritische advies van de Raad van State. Ook de Gegevensbeschermingsautoriteit formuleerde een even streng advies, bijna identiek aan de formulering van de juridische adviesraad van de Raad in Europa. De heer Van Quickenborne stelt dat de minister deze adviezen naast zich neerlegt. De Programmawet, dat voor de zomer 2025 werd gestemd, werd ook ter advies aan de Raad van State voorgelegd. In het wetsontwerp stond aanvankelijk *money control*, maar die bepaling is eruit gehaald. Nu voegt de minister *money control* opnieuw in via een amendement op het voorliggende wetsontwerp diverse bepalingen. Het lid stelt dat de zeven alinea's, opgenomen in een amendement van de regering, uiteraard een uitvoerige bespreking vergen. De oorspronkelijke tekst in de programmawet van voor de zomer en de later ingediende amendementen verschillen door de toevoeging van twee alinea's, waarvan één zonder normatief karakter. Een wetsbepaling zonder normatieve waarde is echter zinloos.

Tot slot benadrukt de spreker dat twee arresten rechtstreeks van toepassing zijn op het wetsontwerp van de minister, namelijk de arresten *Dun & Bradstreet* en *CHUFA*.

Betreffende het negende hoofdstuk, kondigt het lid aan dat hij uitvoerig zal ingaan op het gebruik van artificiële intelligentie binnen de fiscaliteit. Technologie mag enkel worden ingezet wanneer zij vooruitgang bevordert en niet wanneer zij de privacy van burgers onder druk zet. Volgens het commissielid dreigt *money control* technologie te gebruiken op een manier die het privéleven van burgers ernstig schaadt. De heer Van Quickenborne zal de impact van artificiële intelligentie en van de AI-act op *money control* behandelen, aangezien hierover volgens hem in het Parlement nauwelijks debat heeft plaatsgevonden. Ook de werking van *money control* en datamining zal toegelicht worden. Verder zal hij aandacht besteden aan de zogenoemde damfiches, die volgens hem tot de best bewaarde geheimen van de fiscaliteit behoren.

In hoofdstuk 10 bespreekt het commissielid de relatie tussen het CAP, *money control* en het Valentijnsarrest van 14 februari 2013. Hij verwees reeds kort naar dat

ensuite concentré sur quelques dispositions complémentaires du texte législatif, dont l'ajout des crypto-actifs et l'enregistrement des comptes-titres dans le PCC. Il a émis plusieurs réserves à cet égard, puis a procédé à l'examen des sept alinéas figurant dans les amendements du gouvernement, qui fixent les contours du *money control*.

Le membre évoque ensuite à nouveau l'avis critique du Conseil d'État. L'Autorité de protection des données a formulé un avis tout aussi sévère, dont les termes sont quasiment identiques à ceux retenus par le conseil juridique consultatif européen. M. Van Quickenborne affirme que le ministre ignore ces avis. La loi-programme, qui a été votée avant l'été 2025, a également été soumise pour avis au Conseil d'État. Le projet de loi mentionnait initialement le *money control*, mais la disposition y afférente a été supprimée. À présent, le ministre réintroduit le *money control* par le biais d'un amendement au projet de loi à l'examen portant des dispositions diverses. Le membre indique que les sept alinéas figurant dans un amendement du gouvernement nécessitent de toute évidence une discussion approfondie. Le texte mentionné initialement dans la loi-programme d'avant l'été diffère de celui qui intègre les amendements présentés ultérieurement, en raison de l'ajout de deux alinéas, dont l'un n'a pas de caractère normatif. Or, une disposition légale sans valeur normative est dénuée de sens.

Enfin, l'intervenant souligne que deux arrêts s'appliquent directement au projet de loi du ministre, à savoir les arrêts *Dun & Bradstreet* et *CHUFA*.

S'agissant du chapitre 9, le membre indique qu'il abordera en détail le recours à l'intelligence artificielle dans le domaine de la fiscalité. La technologie ne peut être mobilisée que lorsqu'elle favorise le progrès et non lorsqu'elle compromet le respect de la vie privée des citoyens. Le membre considère que le *money control* risque d'utiliser la technologie d'une manière qui porte gravement atteinte à la vie privée des citoyens. M. Van Quickenborne abordera l'impact de l'intelligence artificielle et du Règlement sur l'intelligence artificielle sur le *money control*, puisque, selon lui, ce sujet n'a pratiquement pas été débattu au Parlement. Il commentera également le fonctionnement du *money control* et du *data mining*. Le membre s'intéressera en outre aux fiches *Data & Access Management*, connues sous la dénomination de "fiches DAM", qui font partie, selon lui, des secrets les mieux gardés de la fiscalité.

Dans le chapitre 10, le membre examinera les liens entre le PCC, le *money control* et l'arrêt du 14 février 2013, dit arrêt de la Saint-Valentin. Il a déjà brièvement

arrest en merkt op dat het een relevant toetsingskader vormt voor de beoordeling van *money control*.

Een cruciale vraag die in hoofdstuk 10 behandelt zal worden is de evolutie naar een vermogenskadaster, een onmiskenbaar politiek vraagstuk. Volgens de heer van Quickenborne streven de socialisten ernaar dit wetsontwerp vóór het einde van het jaar 2025 goedgekeurd te krijgen, mede omdat het voortbestaan van de regering onzeker is. Het lid stelt dat de socialisten, indien *money control* niet wordt goedgekeurd, naar eigen zeggen niets hebben om mee uit te pakken bij de kiezer. Indien het wetsontwerp daarentegen wél wordt goedgekeurd, zou dit volgens hem de weg openen naar het vermogenskadaster, een maatregel die de socialistische partij al langer nastreeft.

De spreker kondigt aan dat hij in hoofdstuk 12 de minister enkele handvatten probeert aan te reiken om het probleem op een verantwoorde wijze op te lossen. Daarna volgt in hoofdstuk 13 en de daaropvolgende hoofdstukken het verdere inhoudelijke vervolg en de conclusies.

De heer Van Quickenborne leidt vervolgens hoofdstuk 9 in, waarin hij de effectieve inhoud van de amendementen nrs. 12 tot 22 (DOC 56 0963/005) bespreekt, die voorzien in de wijziging van het Wetboek diverse rechten en taksen om bepaalde ambtenaren toegang te verlenen tot het centraal aanspreekpunt van de Nationale Bank van België. De voorliggende wettekst, ondertussen aangenomen in eerste lezing (DOC 56 0963/020), is tot stand gekomen via amendementen die de minister midden september heeft ingediend. De vele herindieningen en wijzigingen van de amendementen tonen, volgens het commissielid, aan dat binnen de regering aanzienlijke onenigheid bestaat over deze bepalingen.

De bovengenoemde amendementen beogen de artikelen 95/1 tot en met 95/8 in te voegen, waarbij het artikel 95/3, dat uit zeven alinea's bestaat, het meest verregaand is, volgens het commissielid. De amendementen beogen in een eerste luik het toepassingsgebied van het Centraal Aanspreekpunt (CAP) uit te breiden naar cryptoactiva en in een tweede luik de toegang tot het CAP uit te breiden om controles op de jaarlijkse taks op de effectenrekeningen mogelijk te maken, in het bijzonder met het oog op de handhaving van de antimisbruikbepalingen.

Het CAP bevat vandaag reeds een overzicht van de bankrekeningen en bijbehorende saldi van alle Belgen. Die saldi zijn de bedragen die men op een bepaald moment op zijn bankrekening heeft staan. Twee keer per jaar, op 30 juni en 31 december, wordt daarvan een momentopname genomen die wordt gebruikt om

renvoyé à cet arrêt et fait observer qu'il constitue un cadre d'évaluation pertinent du *money control*.

L'évolution vers un cadastre des fortunes est une question cruciale et incontestablement politique qui sera examinée dans le chapitre 10. M. Van Quickenborne indique que les socialistes s'emploient à faire adopter ce projet de loi avant la fin de l'année 2025, notamment en raison de l'incertitude qui pèse sur la survie du gouvernement. Le membre indique que, si le *money control* n'est pas approuvé, les socialistes n'auront, selon leurs propres dires, pas de trophée à présenter aux électeurs. En revanche, si le projet de loi est adopté, la voie menant au cadastre des fortunes serait ouverte. Il s'agit d'une mesure à laquelle le parti socialiste aspire depuis longtemps.

L'intervenant indique qu'il tentera, dans le chapitre 12, d'offrir quelques outils au ministre pour remédier au problème de manière responsable. La suite de ses considérations, ainsi que les conclusions, figureront dans les chapitres 13 et suivants.

M. Van Quickenborne entame ensuite le chapitre 9, dans lequel il examine le contenu effectif des amendements n^{os} 12 à 22 (DOC 56 0963/005) tendant à modifier le Code des droits et taxes divers afin d'octroyer à certains fonctionnaires l'accès au point de contact central de la Banque Nationale de Belgique. Le texte à l'examen, qui a été adopté en première lecture dans l'intervalle (DOC 56 0963/020), est le fruit d'amendements que le ministre a présentés à la mi-septembre. Le membre estime que le fait que ces amendements aient été maintes fois présentés et modifiés révèle qu'un profond désaccord existe au sein du gouvernement au sujet de ces dispositions.

Les amendements précités tendent à insérer les articles 95/1 à 95/8. Parmi ces dispositions, c'est l'article 95/3, qui comprend sept alinéas, qui va le plus loin aux yeux du membre. Les amendements visent, dans un premier volet, à étendre le champ d'application du Point de contact central (PCC) aux crypto-actifs et, dans un deuxième volet, à étendre l'accès au PCC pour permettre les contrôles de la taxe annuelle sur les comptes-titres, en particulier en vue de veiller au respect des dispositions anti-abus.

Le PCC contient déjà actuellement un aperçu des comptes bancaires de tous les Belges, avec les soldes y afférents. Ces soldes correspondent aux montants qui se trouvent sur les comptes bancaires à un moment donné. Deux fois par an, le 30 juin et le 31 décembre, une image instantanée de ces soldes est établie et

de controles binnen het kader van *money control* te verwezenlijken. Wanneer het saldo tussen deze twee data opvallend schommelt, kan de administratie hierover vragen stellen. Dat is de huidige werking van het CAP.

De spreker verduidelijkt dat de regering nu voorstelt om cryptoactiva aan deze verplichting toe te voegen. Dit blijkt uit nieuwe artikel 95/4. Volgens de verantwoording bij artikel 95/4 wordt de aanmeldingsplicht uitgebreid omdat de Europese witwasregelgeving voortaan de registratie van cryptowallets vereist. Cryptoactiva, zo wordt geciteerd, worden vaak gebruikt door criminele organisaties om het traditionele banksysteem te ontwijken en om terroristische activiteiten te financieren. Daarom dringt rapportering via het CAP zich op.

De heer Van Quickenborne merkt op dat het klopt dat cryptoactiva gevoeliger zijn voor misbruik door criminelen dan klassieke cashgelden. Vandaag investeren veel jongeren in beleggingen die bestaan uit bitcoin en andere cryptoactiva. Het commissielid acht het daarom te verregaand om cryptoactiva voornamelijk als misdadig instrument te bestempelen. Kan de minister cijfers bezorgen over het effectieve aandeel van criminele activiteiten binnen het cryptogebruik? Hoe performant is justitie in de bestrijding ervan? Het lid verwijst daarbij naar een recent artikel van onderzoeksjournalist Lars Bové in *De Tijd*, waarin wordt aangehaald dat politie en justitie momenteel onvoldoende uitgerust zijn om cryptocriminaliteit efficiënt te bestrijden. Daarom vraagt het lid verduidelijking over de aanpak van cryptocriminaliteit, de resultaten inzake inbeslagnames en de werking van de Centraal Orgaan voor de Inbeslagneming en Verbeurdverklaring (COIV).

Het lid gaat vervolgens in op de definitie in het wetsontwerp. Volgens de voorgestelde tekst is een cryptoactivarekening een rekening waarop cryptoactiva kunnen worden gecrediteerd of waarvan deze kunnen worden gedebiteerd. Voor de omschrijving van cryptoactiva verwijst het ontwerp naar artikel 2, § 1, 7°, Verordening (EU) 2024/1624 van het Europees Parlement en de Raad van 31 mei 2024 tot voorkoming van het gebruik van het financiële stelsel voor witwassen of terrorismefinanciering, dat op zijn beurt verwijst naar artikel 2, lid 4, van Verordening (EU) 2023/1114 van het Europees Parlement en de Raad van 31 mei 2023 betreffende cryptoactivamarkten.

De heer Van Quickenborne stipt aan dat de *Common Reporting Standard* (CRS) in twee richtingen werkt:

utilisée pour effectuer les contrôles dans le cadre du *money control*. Lorsque le solde observé à ces deux dates varie de manière flagrante, l'administration peut poser des questions. Voilà comment fonctionne le PCC à l'heure actuelle.

L'intervenant précise que le gouvernement propose à présent de soumettre également les crypto-actifs à cette obligation, ainsi qu'il ressort du nouvel article 95/4. Selon la justification relative à l'article 95/4, l'obligation de notification est étendue parce que la réglementation anti-blanchiment européenne exige désormais que les portefeuilles de crypto-actifs soient enregistrés. Il est indiqué dans cette justification que les crypto-actifs sont couramment utilisés par des organisations criminelles pour échapper au système bancaire classique et pour financer des activités terroristes. C'est pourquoi un rapportage par le biais du PCC s'impose.

M. Van Quickenborne fait observer qu'il est exact que les crypto-actifs sont plus vulnérables au détournement par des criminels que l'argent liquide classique. Mais aujourd'hui, de nombreux jeunes investissent dans des placements de bitcoins et d'autres crypto-actifs. Le membre estime dès lors qu'il est excessif de considérer les crypto-actifs comme un instrument essentiellement criminel. Le ministre pourrait-il fournir des chiffres concernant la part effective des activités criminelles dans l'utilisation des crypto-actifs? La Justice est-elle performante dans la lutte contre cette criminalité? Le membre renvoie à cet égard à un article récent du journaliste d'investigation Lars Bové publié dans *De Tijd*, qui constate que la police et la Justice ne sont aujourd'hui pas suffisamment équipées pour lutter efficacement contre la cryptocriminalité. C'est pourquoi le membre demande des précisions en ce qui concerne la lutte contre ce type de criminalité, les résultats en matière de saisies et le fonctionnement de l'Organe central pour la saisie et la confiscation (OCSC).

Le membre aborde ensuite la définition figurant dans le projet de loi. Selon le texte proposé, un compte de crypto-actifs est un compte sur lequel des crypto-actifs peuvent être crédités ou duquel ces crypto-actifs peuvent être débités. S'agissant de la définition des crypto-actifs, le projet renvoie à l'article 2, § 1^{er}, 7), du règlement (UE) 2024/1624 du Parlement européen et du Conseil du 31 mai 2024 relatif à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, lequel renvoie à son tour à l'article 2, paragraphe 4, du règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de crypto-actifs.

M. Van Quickenborne souligne que le dispositif *Common Reporting Standard* (CRS) fonctionne dans

buitenlands vermogen van Belgische inwoners moet in België worden aangegeven, zoals bepaald in het wetsontwerp. De gegevensoverdracht in de andere richting – namelijk over activa die in België worden aangehouden door niet-ingezetenen, zoals Duitsers – is echter niet opgenomen in de amendementen van de Arizone-meerderheid. Komt er ook een gegevensoverdracht voor activa die door niet-ingezetenen worden aangehouden in België?

Het lid verwijst vervolgens naar de aangifte van rekeningen van videospelletjes waarin het regeerakkoord voorziet, maar waarover in het wetsontwerp of in de amendementen niet wordt gerept. Verwijzend naar de artikelen 95/4 en 95/5 vraagt hij wanneer die maatregel daadwerkelijk zal worden toegepast.

Aangaande de effectentaks merkt de heer Van Quickenborne op dat effectenrekeningen zullen worden opgenomen in het Centraal Aanspreekpunt van rekeningen en financiële contacten (CAP). Op dit moment moet er een vermoeden van fraude zijn om toegang tot het CAP te krijgen. Met het wetsontwerp wordt het mogelijk om, specifiek voor de effectentaks, die toegang te krijgen zonder vermoeden van fraude. Ter rechtvaardiging daarvan wordt aangevoerd dat het noodzakelijk is de specifieke antimisbruikbepalingen te controleren en te voorkomen dat de waarde van de rekeningen onder de drempel van 1 miljoen euro zakt.

De heer Van Quickenborne uit zijn bedenkingen over die wijziging. Hij meent dat wie die taks moet betalen, minder garanties geniet dan andere belastingplichtigen. Hij vindt de aanpak van de regering coherent noch objectief, aangezien voor andere belastingen ook antimisbruikmaatregelen met een vermoeden van fraude gelden.

De spreker herinnert eraan dat volgens de GBA de toegang tot het CAP gericht en specifiek moet blijven en dat de gegevens alleen mogen worden geraadpleegd bij vermoedens van fraude of belastingontwijking. Volgens het lid dreigt de maatregel de gegevensbescherming te verzwakken. Zodra toegang wordt verleend voor de effectentaks, zal de administratie de informatie moeten delen met andere diensten, overeenkomstig de artikelen 335 en 336 van het Wetboek van de inkomstenbelastingen (WIB) en de bepalingen van het Wetboek diverse rechten en taksen.

De heer Van Quickenborne wijst op het ontbreken van een regeling voor de uitgaande CRS, het feit dat de aangifte van elektronische kansspelrekeningen niet geïntegreerd is, de twijfelachtige verantwoording van de toegang tot het CAP voor de taks op de effectenrekeningen zonder vermoeden van fraude, en de ontoereikende en inconsistente garanties voor gegevensbescherming.

les deux sens: les actifs détenus à l'étranger par des résidents belges doivent être déclarés en Belgique, ce qui est prévu par le projet de loi. Toutefois, la transmission dans l'autre sens – à savoir des actifs détenus en Belgique par des non-résidents, comme des Allemands – n'est pas prévue dans les amendements proposés par la majorité Arizona. L'orateur s'interroge: est-il prévu d'appliquer également une transmission pour des actifs détenus en Belgique par des non-résidents?

Le membre évoque ensuite la déclaration des comptes de jeux électroniques prévue dans l'Accord de gouvernement, qui n'apparaît pas dans le projet de loi ni dans les amendements, et demande quand cette mesure sera effectivement appliquée, en se référant aux articles 95/4 et 95/5.

Concernant la taxe sur les comptes-titres, M. Van Quickenborne précise que les comptes-titres seront intégrés au Point de contact central des comptes et contrats financiers (PCC). Actuellement, l'accès au PCC pour les contrôles fiscaux nécessite une suspicion de fraude. Le projet de loi permet, pour la taxe sur les comptes-titres, l'accès sans aucune suspicion de fraude. C'est justifié par la nécessité de contrôler les dispositions anti-abus spécifiques afin d'éviter que la valeur des comptes ne tombe en dessous du seuil de 1 million d'euros.

M. Van Quickenborne critique cette modification et estime que les contribuables soumis à cette taxe bénéficient de moins de garanties que les autres et que la logique du gouvernement n'est ni cohérente ni objectivée, puisque d'autres impôts possèdent également des mesures anti-abus avec suspicion de fraude.

L'orateur rappelle que l'APD souligne que l'accès au PCC doit rester ciblé et spécifique, et que les données ne doivent être consultées qu'en cas de suspicions de fraude ou d'évasion fiscale. Selon le député, la mesure risque d'affaiblir la protection des données: une fois l'accès donné pour la taxe sur les comptes-titres, l'administration devra partager ces informations avec d'autres services, conformément aux articles 335 et 336 du Code des impôts sur les revenus (CIR) et aux dispositions du Code des droits et taxes divers.

M. Van Quickenborne insiste sur l'absence de dispositif pour le CRS sortant, la non-intégration de la déclaration des comptes de jeux électroniques, la justification contestable de l'accès au PCC pour la taxe sur les comptes-titres sans soupçon de fraude, et les garanties de protection des données insuffisantes et incohérentes. Il demande au ministre de clarifier ces

Hij vraagt de minister die punten te verduidelijken en toe te lichten hoe het wetsontwerp de CRS-regels en de rechten van de belastingplichtigen in acht neemt.

De spreker gaat vervolgens nader in op het deel van het wetsontwerp dat betrekking heeft op de afschaffing van bepaalde taksen. Hij keurt die maatregelen goed en laat weten dat zijn fractie ze zal steunen, al stelt hij wel voor om nog meer taksen af te schaffen. Daartoe heeft hij overigens amendementen ingediend.

Met betrekking tot de bescherming van gegevens in verband met *money control* herinnert de spreker eraan dat de artikelen 12 en 11, § 2, van het Wetboek diverse rechten en taksen bepalen dat alle informatie die een ambtenaar in de uitoefening van zijn ambt verkrijgt, kan worden gebruikt om verschuldigde belastingbedragen op te sporen. Door een uitgebreide toegang tot het CAP toe te staan, slaat de minister dus een bres in de wetgeving die de vertrouwelijkheid van de bankgegevens beschermt. Een raadpleging die aanvankelijk beperkt is tot fraude, zou via dat mechanisme namelijk kunnen leiden tot een breed toegepaste informatie-uitwisseling tussen overheidsdiensten, waardoor de bestaande waarborgen hun betekenis verliezen.

Het lid benadrukt voorts dat het systeem van *money control* wettelijk niet beperkt is tot georganiseerde fraude, in weerwil van wat de minister beweert. Hij stelt vast dat de wet geen enkel onderscheid maakt en het gebruik ervan voor alle vormen van fraude toestaat. De heer Van Quickenborne geeft een reeks concrete voorbeelden om aan te tonen dat gewone burgers, zonder enige frauduleuze intentie, onderworpen kunnen worden aan controles omdat hun bankrekening een atypische beweging registreert. Hij haalt het voorbeeld aan van een dame die een onverwachte erfenis ontvangt van een oudtante met wie zij niet veel contact meer had, of van broers die hun ouderlijk huis verkopen en een hoger bedrag krijgen dan verwacht, of nog van iemand die een televisiespel wint en een aanzienlijke geldprijs ontvangt. Volgens de spreker tonen dergelijke situaties aan dat elke burger een potentiële verdachte wordt die elke ongewone geldstroom moet verantwoorden.

In het bijzonder hekelt de heer Van Quickenborne dat het fundamentele principe dat de overheid bankgegevens alleen mag raadplegen bij vermoedens van fraude, overboord gaat. In het nieuwe systeem zullen alle bankgegevens van alle Belgen standaard worden gecontroleerd, teneinde afwijkingen vast te stellen en daar vervolgens een verklaring voor te eisen. Volgens de spreker wordt de bewijslast zo omgekeerd en worden alle burgers beschouwd als vermeende fraudeurs.

points et d'expliquer la conformité du projet aux règles CRS et aux droits des contribuables.

L'orateur en vient à la partie du projet de loi relative à la suppression de certaines taxes. Il approuve ces mesures et annonce que son groupe les soutient, même s'il propose de supprimer davantage de taxes. Il a d'ailleurs déposé des amendements en ce sens.

Concernant la protection des données liées au dispositif "*money control*", l'orateur rappelle que les articles 12 et 11, § 2 du Code des droits et taxes divers prévoient que toute information obtenue par un fonctionnaire dans l'exercice de ses fonctions peut être utilisée pour rechercher des sommes dues au titre d'un impôt. Dès lors, en autorisant l'accès élargi au point de contact central (PCC), le ministre ouvre une brèche dans une législation qui protégeait la confidentialité des données bancaires, puisqu'une consultation initialement limitée à la fraude pourrait mener, via ce mécanisme, à un partage généralisé d'information entre administrations, vidant de leur substance les garanties existantes.

Le député souligne ensuite que le dispositif "*money control*" n'est pas limité, en droit, à la seule fraude organisée, contrairement à ce qu'affirme le ministre. Il constate que la loi ne prévoit aucune distinction et permet une utilisation pour toute forme de fraude. M. Van Quickenborne donne une série d'exemples concrets afin de montrer que des citoyens ordinaires, sans aucune intention frauduleuse, pourraient être soumis à des contrôles parce que leur compte bancaire enregistre un mouvement atypique. L'orateur évoque le cas d'une dame bénéficiant d'un héritage inattendu d'une grand-tante avec qui elle n'avait plus beaucoup de contact, des frères qui obtiennent une somme plus élevée que prévu en vendant l'immeuble familial, une personne qui gagne un jeu de télévision et obtient un gain important. Selon l'intervenant, ces situations démontrent que tout citoyen devient un suspect potentiel devant justifier tout flux financier inhabituel.

M. Van Quickenborne critique, en particulier, le renversement du principe fondamental selon lequel l'administration ne peut consulter les données bancaires qu'en présence d'une suspicion de fraude. Le nouveau système prévoit un contrôle systématique de toutes les données bancaires de tous les Belges, afin d'identifier des anomalies et d'exiger ensuite des explications. Pour l'orateur, il s'agit d'une inversion de la charge de la preuve et d'une assimilation généralisée des citoyens à des fraudeurs présumés.

De spreker vraagt de minister waarom er geen waarborgen zijn ingebouwd om te voorkomen dat de onder het mom van *money control* geraadpleegde gegevens meteen worden hergebruikt door andere fiscale diensten, op grond van de in de artikelen 335 en 336 van het WIB geregelde verplichtingen inzake informatie-uitwisseling. De heer Van Quickenborne zegt bereid te zijn een amendement op te stellen om die informatiedeling duidelijk af te bakenen, maar stelt vast dat de minister elk amendement van de oppositie stelselmatig terzijde schuift. De spreker herbevestigt dat zijn fractie zich fel zal kanten tegen de in uitzicht gestelde wet, die volgens hem een aanslag is op de persoonlijke levenssfeer van de burgers. De heer van Quickenborne herhaalt zijn vergelijking met huiselijk geweld: iedereen is ertegen, maar dat wil nog niet zeggen dat men een camera moet hangen in de slaapkamer van elke burger. Volgens de spreker valt die redenering perfect door te trekken naar deze kwestie: fiscale fraude bestrijden is uiteraard een goede zaak, maar dat betekent niet dat elke burger zomaar moet worden gescreend.

Vervolgens stipt de spreker amendement nr. 16 (DOC 56 0963/005) aan, dat bepalingen bevat om het in 2011 opgerichte CAP grondig te hervormen. De spreker leest en becommentarieert de op 17 september ingediende amendementen. Die geven de overheid de mogelijkheid alle CAP-gegevens over te hevelen naar een datawarehouse, teneinde er datamining, datamatching en profilering op toe te passen. Hij legt de nadruk op profilering, een praktijk die in artikel 4.4 van de AVG wordt gedefinieerd en die onvermijdelijk een vorm van automatische verwerking veronderstelt. Dat wil dus zeggen dat het wetsontwerp, dat profilering toelaat, niet strookt met de bewering van de minister dat het systeem geen geautomatiseerde algoritmes zou gebruiken.

Vervolgens analyseert de spreker de juridische strekking van het eerste lid, dat uitdrukkelijk afwijkt van artikel 322 van het WIB. Die bepaling heft een aantal essentiële waarborgen op, met name de gerichtheid van informatieverzoeken, de motivering en de eerbiediging van het beroepsgeheim. Zo verwordt het CAP tot een datareservoir dat altijd, zonder rechterlijke toestemming of voorafgaand vermoeden, toegankelijk is.

De heer Van Quickenborne benadrukt ook dat de heel ruime verwijzing naar de taken van de belastingdienst – inning, invordering en controle van de belastingen – de deur openzet voor onbeperkt gebruik van gegevens. Die formulering, in combinatie met het ontbreken van grensbedragen, maakt het mogelijk de informatie van alle belastingplichtigen te gebruiken, ongeacht het bedrag. De spreker ziet hierin een ingrijpende transformatie van

L'intervenant interroge le ministre sur l'absence de garanties empêchant que les données consultées dans le cadre du "*money control*" soient immédiatement réutilisées par d'autres services fiscaux par application des obligations de partage de l'information prévues aux articles 335 et 336 du CIR. M. Van Quickenborne indique être disposé à rédiger un amendement pour encadrer formellement ce partage d'informations, tout en constatant que le ministre refuse systématiquement tout amendement émanant de l'opposition. L'orateur réaffirme que son groupe s'opposera fermement au texte, qu'il juge attentatoire à la vie privée des citoyens. M. Van Quickenborne reprend sa comparaison avec la violence domestique: ce n'est pas parce que tout le monde est opposé à la violence domestique qu'il faille mettre une caméra dans la chambre à coucher des citoyens. Pour M. Van Quickenborne, c'est exactement le même raisonnement qu'il convient d'appliquer ici: ce n'est pas parce qu'il convient de lutter contre la fraude fiscale qu'il faille procéder à un screening de tous les citoyens.

Le député en vient à l'amendement n° 16 (DOC 56 0963/005), qui contient des alinéas réformant en profondeur le PCC, créé en 2011. L'intervenant lit et commente ces amendements déposés le 17 septembre, qui introduisent la possibilité pour l'administration d'utiliser toutes les données du PCC pour les intégrer dans un "datawarehouse" et mener des opérations de "*data mining*", "*datamatching*" et de profilage. Il insiste sur l'importance du terme "profilage", défini à l'article 4.4 du RGPD, qui implique nécessairement une forme de traitement automatisé. L'orateur relève donc une contradiction entre le texte, qui autorise le profilage, et les déclarations du ministre affirmant que le système ne repose pas sur des algorithmes automatisés.

L'orateur analyse ensuite la portée juridique du premier alinéa, qui déroge explicitement à l'article 322 du Code des impôts sur les revenus. Selon lui, cette disposition supprime des garanties essentielles: le caractère ciblé des demandes d'information, la motivation et le respect du secret professionnel. Cette disposition transforme donc le PCC en un réservoir de données accessible systématiquement, sans autorisation judiciaire ni suspicion préalable.

M. Van Quickenborne souligne aussi que la référence très large aux "missions de l'administration" – perception, recouvrement et contrôle de l'impôt – ouvre la voie à une utilisation illimitée des données. Cette formulation, combinée à l'absence de seuils, permet l'exploitation des informations de tous les contribuables, indépendamment du montant en jeu. L'orateur estime qu'il s'agit d'une transformation majeure du droit fiscal, équivalant

het fiscaal recht, een heuse juridische revolutie die het beginsel van de goede trouw van de belastingplichtige afvoert.

De spreker buigt zich over de reikwijdte van het eerste lid en is van mening dat die bepaling het pad effent naar een regeling voor de profilering van individuen en ondernemingen op basis van de waarschijnlijkheid dat ze fraude plegen. Die keuze is problematisch daar ze betekent dat elke burger een risico-indicator krijgt toegewezen, wat niet te verenigen valt met de grondbeginselen van de rechtsstaat.

De heer Van Quickenborne wijst er verder op dat elk afwijkend gebruik van beschermde persoonsgegevens strikt bij wet moet worden gedefinieerd. De spreker stipt aan dat de Grondwet, de AVG en de Europese rechtspraak vereisen dat een uitzondering op de gegevensbescherming nauwgezet wordt omschreven, zowel qua doeleinden als qua gegevenscategorieën. Het eerste lid maakt toegang tot alle gegevens mogelijk voor alle doeleinden die verband houden met fraudebestrijding, zonder materiële of temporele beperkingen. Hij bestempelt die aanpak als een blanco cheque, als een algemene delegatie, wat juridisch ontoelaatbaar is.

De spreker verwijst vervolgens naar artikel 22 van de AVG, dat geautomatiseerde beslissingen met juridische of voor iedereen gelijkaardige gevolgen verbiedt. Voormeld lid staat profilering echter uitdrukkelijk toe, hoewel dat een verboden vorm van geautomatiseerde beslissing is. De spreker benadrukt dat het niet om een technisch detail gaat, maar om een rechtstreeks conflict tussen de AVG en de inhoud van het wetsontwerp.

De heer Van Quickenborne schraagt die analyse met rechtspraak van het Hof van Justitie van de Europese Unie en overloopt de arresten *Digital Rights Ireland*, *Tele2 Sverige* en *La Quadrature du Net*. Hij herinnert eraan dat het Hof systematisch elke veralgemeende en ongedifferentieerde verzameling of bewaring van persoonsgegevens veroordeelt omdat het die onevenredig acht. Hij merkt op dat het bewuste lid uitgerekend in dat soort veralgemeende inzameling voorziet, zonder een specifieke doelgroep af te bakenen of geïndividualiseerd te werk te gaan.

Hij legt vervolgens uit dat de in het lid vervatte regeling in de interne rechtsorde het effect van een *lex specialis* heeft. Zodra ze wordt aangenomen, overrulet ze immers *de facto* de waarborgen die door sectorale wetgeving worden geboden – het Wetboek van de inkomstenbelastingen, de btw-wetgeving, de douaneregelgeving – en vooral dan de vereisten inzake evenredigheid, motivering, eerbiediging van het beroepsgeheim en voorafgaande

à une “révolution juridique” et renversant le principe du contribuable présumé de bonne foi.

L'intervenant examine la portée du premier alinéa et considère que celui-ci instaure la possibilité de mettre en place un système destiné à profiler individus et entreprises sur la base d'une probabilité de fraude. Il juge cette orientation problématique, parce qu'elle revient à attribuer à chaque citoyen un indicateur de risque, ce qui n'est pas compatible avec les principes fondamentaux de l'État de droit.

M. Van Quickenborne poursuit en rappelant que toute utilisation dérogatoire de données personnelles protégées doit être strictement définie par la loi. L'orateur indique que la Constitution, le RGPD et la jurisprudence européenne exigent qu'une exception à la protection des données soit prévue de manière précise, tant quant aux finalités que quant aux catégories de données concernées. Or l'alinéa ouvre l'accès à toutes les données pour tous les objectifs liés à la lutte contre la fraude, sans limitation matérielle ni temporelle. Il qualifie ce mécanisme de chèque en blanc: une délégation générale, qui est inadmissible juridiquement.

L'orateur se réfère ensuite au RGPD, en rappelant que l'article 22 interdit les décisions automatisées ayant des effets juridiques ou similaires sur les personnes. Or, l'alinéa autorise explicitement le profilage, ce qui constitue une forme de décision automatisée interdite. L'intervenant souligne qu'il ne s'agit pas d'un détail technique, mais d'un conflit direct entre le RGPD et le contenu du projet.

M. Van Quickenborne étaye cette analyse par la jurisprudence de la Cour de justice de l'Union européenne et passe en revue les arrêts suivants: “*Digital Rights Ireland*”, “*Tele2 Sverige*” et “*La Quadrature du Net*”. Il rappelle que la Cour condamne systématiquement toute collecte ou conservation généralisée et indifférenciée de données personnelles, considérée comme disproportionnée. Le député constate que l'alinéa organise précisément ce type de collecte généralisée, sans ciblage et sans fondement individualisé.

L'intervenant explique ensuite que, sur le plan interne, cet alinéa fonctionne comme une *lex specialis*. Une fois adopté, cet alinéa écarte, *de facto*, les garanties prévues par les législations sectorielles – le Code des impôts sur les revenus, la législation TVA, la réglementation douanière – notamment les exigences de proportionnalité, de motivation, de respect du secret professionnel et de contrôle préalable. Dès lors que l'opération est qualifiée

controle. Zodra de bewerking als datamining of profilering wordt aangemerkt, vervallen die beschermingen immers.

De heer Van Quickenborne heeft het vervolgens over de integratie van de CAP-gegevens in het datawarehouse van de administratie. Ten eerste wijst hij erop dat dat datawarehouse al een enorme hoeveelheid gegevens bevat: aangiftes van de personenbelasting en van de vennootschapsbelasting, btw-aangiftes, RIZIV-informatie, kadastergegevens en gegevens die vanuit het buitenland worden verzonden in het kader van FATCA (*Foreign Account Tax Compliance*), de richtlijn betreffende de administratieve samenwerking (DAC) en het CRS-systeem. Hij beklemtoont dat de meeste van die gegevens afkomstig zijn van vrijwillige aangiftes of van automatische uitwisselingen binnen een vastgesteld kader. Omgekeerd kunnen de CAP-gegevens vandaag alleen worden geraadpleegd in gevallen van een voorafgaand vermoeden. Het bewuste lid verstoort dat evenwicht doordat het die gegevens veralgemeend opneemt, waardoor het intrusierisico sterk toeneemt en het datawarehouse verwordt tot een systeem dat vergelijkbaar is met een *Passenger Name Record*-bestand (PNR), maar dan toepasbaar op de hele bevolking.

Vervolgens staat hij stil bij de waarborgen die de AVG voor profilering oplegt: de gegevensverwerking moet transparant zijn, de beslissingen vergen een menselijke interventie, er moet een volwaardige beroepsmogelijkheid zijn en de verwerking moet strikt tot de noodzakelijke gegevens beperkt blijven. Hij merkt op dat geen van die waarborgen in de tekst is opgenomen en besluit daaruit dat de wettelijke erkenning van profilering zonder ook maar enige bescherming gepaard gaat, waardoor ze onbestaanbaar is met het Europees recht.

De spreker gaat in op de systemische weerslag van dat lid. Volgens de heer Van Quickenborne wordt de FOD Financiën de bevoegdheid verleend om de hele bevolking grondig en voortdurend te screenen, zonder voorafgaande reden, zonder gerechtelijke controle en zonder het principe van hoor en wederhoor in acht te nemen. Zo wordt de belastingdienst bijna een inlichtingendienst, wat veel verder gaat dan de gebruikelijke fiscale inning en controle. De spreker voegt eraan toe dat bepaalde ambtenaren rechtstreeks toegang hebben tot de gegevens van het CAP, waardoor een groep "gegevensambtenaren" ontstaat met meer macht dan een onderzoeksrechter, die onderworpen blijft aan gerechtelijke controle.

Ter afsluiting van zijn betoog toetst de heer Van Quickenborne het lid aan de grondwettelijke vereisten. Om te beginnen stelt hij een schending van het legaliteitsbeginsel vast, aangezien de wet onvoldoende nauwkeurig en voorspelbaar is. Vervolgens wijst hij

de *data mining* ou de profilage, ces protections cessent d'être applicables.

M. Van Quickenborne aborde alors la question de l'intégration des données du PCC dans le *data warehouse* de l'administration. Il rappelle d'abord que ce *data warehouse* contient déjà une vaste quantité de données: déclarations IPP et ISoc, déclarations TVA, informations ONSS, données du cadastre et données transmises par l'étranger dans le cadre de FATCA (*Foreign Account Tax Compliance*), de la Directive relative à la coopération administrative (DAC – Directive on Administrative Cooperation) et du système CRS. Il souligne que ces données proviennent, pour la plupart, de déclarations volontaires ou d'échanges automatiques encadrés. À l'inverse, les données du PCC ne peuvent être consultées aujourd'hui qu'en cas de suspicion préalable. L'alinéa rompt cet équilibre en intégrant ces données de manière générale, augmentant fortement l'intrusion et transformant le *data warehouse* en un système comparable à un fichier PNR appliqué à l'ensemble de la population.

Il s'arrête ensuite sur les garanties que le RGPD impose pour le profilage: la transparence du traitement, l'intervention humaine dans la prise de décision, la possibilité d'un recours effectif et la limitation stricte aux données nécessaires. Il constate que le texte n'intègre aucune de ces garanties et en conclut que la reconnaissance législative du profilage se fait en l'absence totale de protections, ce qui la rend incompatible avec le droit européen.

L'orateur examine les effets systémiques de l'alinéa. Selon M. Van Quickenborne, le SPF Finances acquiert une capacité d'analyse exhaustive et permanente de l'ensemble de la population, sans cause préalable, sans contrôle juridictionnel et sans respect du principe du contradictoire. Cela confère à l'administration une fonction de quasi-renseignement, excédant son rôle traditionnel de perception et de contrôle fiscal. Il ajoute que certains fonctionnaires désignés bénéficient d'un accès direct aux données du PCC, ce qui crée un cercle d'"agents de données" exerçant un pouvoir supérieur à celui d'un juge d'instruction qui, lui, reste soumis au contrôle judiciaire.

M. Van Quickenborne termine son raisonnement en confrontant l'alinéa aux exigences constitutionnelles. Il note d'abord une atteinte au principe de légalité, la loi manquant de précision et de prévisibilité. L'intervenant constate ensuite une violation du principe

op een schending van het evenredigheidsbeginsel, aangezien de inbreuk op de persoonlijke levenssfeer de gehele bevolking betreft en niet alleen de personen bij wie een risico op fraude bestaat. Tot slot verwijst de spreker naar de scheiding der machten: de belastingdienst krijgt een onderzoeksbevoegdheid die dermate ver reikt dat de prerogatieven van de rechterlijke macht worden aangetast.

De heer Van Quickenborne kan alleen maar vaststellen dat het eerste lid van de tekst, zelfs los van de daaropvolgende leden, al fundamentele problemen oplevert op het stuk van bestaanbaarheid met de Grondwet, de AVG en de rechtspraak van het Hof van Justitie.

De spreker merkt op dat het fundamenteel probleem reeds in het eerste lid van de nieuwe paragraaf 3 van artikel 5 van de wet van 3 augustus 2012 houdende bepalingen betreffende de verwerking van persoonsgegevens door de Federale Overheidsdienst Financiën in het kader van zijn opdrachten (art. 95/3 van de artikelen aangenomen in eerste lezing van het wetsontwerp DOC 56 0963.020) besloten ligt. De bestaande sectorale wetgeving wordt immers opengebroken. Voorts wordt er een structurele en niet-individuele toegang tot het centraal aanspreekpunt van rekeningen en financiële contracten (CAP) verleend. Een derde probleem is volgens hem dat profilering tot een legaal instrument van fiscale controle wordt verheven. De proportionaliteit ten aanzien van het recht op privacy wordt eveneens ondergraven. De logica van controle wordt ook verschoven van feiten naar voorspellingen. Aldus wordt in strijd met de Europese rechtspraak een systeem van massale financiële surveillance gelegitimeerd. Deze fundamentele bezwaren kunnen volgens het lid niet zomaar worden weggeredeneerd.

De heer Van Quickenborne onderstreept dat zijn fractie op dit punt onverzettelijk is, niet omdat het slechts om technische fiscale bepalingen gaat, maar omdat het een constitutionele mijlpaal vormt. Immers, de Belgische wetgever erkent hiermee voor het eerst expliciet dat de fiscus geautomatiseerde risicoprofilering mag uitvoeren op basis van bancaire gegevens van burgers, inclusief minderjarigen, zonder individuele verdenking en met de mogelijkheid tot wat hij omschrijft als "identiteitsontsluiering".

De spreker benadrukt dat het eerste lid van paragraaf 3 een scharnierbepaling vormt. De combinatie van de woorden "rechtstreeks", "alle gegevens", "samenvoegen" en "profilering" creëert volgens hem een nieuwe grammatica van de macht. De burger wordt hierdoor niet langer als persoon maar als dataset wordt beschouwd. Een permanente, geautomatiseerde financiële observatie wordt onder de vlag van risicobeheer

de proportionaliteit, l'ingérence dans la vie privée s'appliquant à l'ensemble de la population, et non aux seules personnes présentant un risque de fraude. Enfin, l'orateur évoque la séparation des pouvoirs: l'administration fiscale se voit attribuer une compétence d'enquête d'une ampleur telle qu'elle empiète sur les prérogatives du pouvoir judiciaire.

M. Van Quickenborne conclut que, dès ce premier alinéa, le texte pose des problèmes fondamentaux de compatibilité avec la Constitution, le RGPD et la jurisprudence de la Cour de justice, indépendamment même des alinéas suivants.

L'intervenant relève que le problème fondamental se trouve déjà dans l'alinéa 1^{er} du nouveau § 3 de l'article 5 de la loi du 3 août 2012 portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions (art. 95/3 des articles adoptés en premier lecture du projet de loi, voir DOC 56 0963.020). En effet, cette disposition en projet déconstruit la législation sectorielle existante. En outre, elle accorde un accès structurel et non individuel au Point de contact central des comptes et contrats financiers (PCC). Selon le membre, un autre problème réside dans le profilage, qui est érigé en instrument légal de contrôle fiscal. La proportionnalité au regard du droit à la vie privée est également érodée. De plus, la logique du contrôle est déplacée du domaine des faits à celui des prévisions. Un système de surveillance financière massive est ainsi légitimé, en contradiction avec la jurisprudence européenne. Selon le membre, ces objections fondamentales ne peuvent pas être purement et simplement réfutées.

M. Van Quickenborne souligne que son groupe est inflexible sur ce point, parce qu'il ne s'agit pas seulement de dispositions fiscales techniques, mais bien d'un jalon constitutionnel. En effet, le législateur belge reconnaît ainsi explicitement pour la première fois que l'administration est autorisée à réaliser un profilage des risques automatisé à partir des données bancaires des citoyens, y compris des mineurs, sans suspicion individuelle et avec une possibilité de dépseudonymisation.

L'intervenant souligne que l'alinéa 1^{er} du § 3 constitue une disposition charnière. Selon lui, la combinaison des mots "directement", "toutes les données", "intégrer" et "profilage" crée une nouvelle grammaire du pouvoir. Le citoyen n'est dès lors plus considéré comme une personne, mais comme un ensemble de données. Sous couvert de gestion des risques, le projet légitimise une observation financière permanente et automatisée. Un

gelegitimeerd. Dergelijke handelswijze is dan ook in strijd met de artikelen 8 en 22 van het EVRM en met de Europese rechtspraak die hij eerder heeft aangehaald. De burger wordt in dit systeem niet meer gecontroleerd omdat hij iets deed maar omdat hij iets zou kunnen doen, wat de essentie van het concept *money control* is.

Wat het tweede lid betreft, vat hij samen dat gegevens in het datawarehouse niet langer worden bewaard dan noodzakelijk, met een maximum van één jaar na de verjaring van alle vorderingen, na de definitieve beëindiging van alle procedures en na de volledige betaling van de verschuldigde bedragen. Hij merkt echter op dat artikel 5, e), van de AVG concrete, doelgebonden bewaartermijnen vereist. De drie cumulatieve voorwaarden — verjaring, definitieve procedure-afsluiting en volledige betaling — kunnen ertoe leiden dat gegevens twintig tot dertig jaar worden bewaard. Dit vormt niet de kortst mogelijke maar de langst mogelijke bewaartermijn.

Hij merkt verder op dat de verwijzing naar alle vorderingen die tot de bevoegdheid van de verwerkingsverantwoordelijke behoren ruim kan worden geïnterpreteerd, namelijk als alle vorderingen van de FOD Financiën in het algemeen en niet uitsluitend met betrekking tot de betrokken belastingplichtige. De spreker wijst erop dat de fiscale verjaring variabel is en in veel gevallen tien jaar bedraagt, wat in de praktijk tot nog langere bewaartermijnen zal leiden. Het gevolg is dus een onvoorzienbare en zeer lange opslag van gegevens in het datawarehouse.

De heer Van Quickenborne vestigt vervolgens de aandacht van de leden op de verwijzing in het tweede lid naar artikel 89 van de AVG. Hij legt uit dat dit artikel derogaties bevat voor archivering in het algemeen belang, voor wetenschappelijk of historisch onderzoek en voor statistische verwerkingen maar slechts mits passende waarborgen zoals pseudonimisering, dataminimalisatie en toegangsbeperking. Het wetsontwerp specificeert volgens hem echter geen bijkomende waarborgen, geen scheiding van doeleinden en geen governance. Daardoor kan artikel 89 in de praktijk dienen om nagenoeg onbeperkte secundaire opslag van profielen en scores te legitimeren. Hij stelt voorts vast dat ook de verplichting om gegevens niet langer te bewaren dan noodzakelijk onvoldoende is uitgewerkt in het wetsontwerp. Het gevolg is een oncontroleerbaar beleid.

Vervolgens gaat hij in op de profileringsdata, features en modelparameters. De bepaling heeft het over persoonsgegevens die voortkomen uit verwerkingen in

tel procédé est dès lors contraire aux articles 8 et 22 de la CEDH et à la jurisprudence européenne que le membre a citée auparavant. Dans ce système, le citoyen n'est plus contrôlé parce qu'il a fait quelque chose, mais parce qu'il pourrait faire quelque chose; c'est l'essence même de la notion de *money control*.

En ce qui concerne l'alinéa 2, il dispose, en résumé, que les données contenues dans le *datawarehouse* ne sont pas conservées plus longtemps que nécessaire, avec une durée maximale de conservation d'un an après la prescription de toutes les actions, après la cessation définitive de toutes les procédures et après le paiement intégral des montants dus. L'intervenant signale toutefois que l'article 5, e), du RGPD impose des délais de conservation concrets et liés aux finalités. Les trois conditions cumulatives (prescription, cessation définitive des procédures et paiement intégral) peuvent avoir pour effet que les données seront conservées pendant vingt ans, voire trente. Il ne s'agit pas du délai de conservation le plus court possible, mais du plus long possible.

L'intervenant relève ensuite que le renvoi à "toutes les actions qui relèvent de la compétence du responsable du traitement" peut être interprété de manière large, à savoir comme toutes les actions du SPF Finances en général et non celles qui visent exclusivement le contribuable concerné. Le député indique que le délai de prescription fiscale est variable et atteint dix ans dans de nombreux cas, ce qui donnera lieu à des délais de conservation encore plus longs dans la pratique. Il en résultera donc un stockage de données dans le *datawarehouse* imprévisible et de très longue durée.

M. Van Quickenborne attire ensuite l'attention des membres sur la référence à l'article 89 du RGPD, qui est faite à l'alinéa 2. Il explique que cet article prévoit des dérogations applicables au traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, mais uniquement moyennant des garanties adéquates telles que la pseudonymisation, la minimisation des données et la limitation de l'accès. Selon le membre, le projet de loi ne précise toutefois ni garantie supplémentaire, ni séparation des finalités, ni gouvernance. Dans la pratique, la référence à l'article 89 peut ainsi servir à légitimer un stockage secondaire pratiquement illimité des profils et des scores de risque. Le député constate également que l'obligation de ne pas conserver les données plus longtemps que nécessaire n'est pas suffisamment développée dans le projet de loi. Il en résulte une politique incontrôlable.

L'intervenant aborde ensuite les données de profilage, les variables et les paramètres du modèle. La disposition concerne des données à caractère personnel

het datawarehouse, inclusief afgeleide gegevens zoals scores, features en labels. Er wordt in geen kortere bewaartermijn voorzien voor onder meer risicoscores, die per definitie voorlopig zijn. Er bestaat volgens hem geen systeem waarbij scores automatisch vervallen en ook geen mechanisme voor model unlearning wanneer trainingsdata worden gewist. Hij wijst erop dat modelparameters die uit persoonsgegevens zijn geleerd, persoonsgegevens kunnen blijven wanneer ze herleidbaar zijn of bias kunnen produceren. Over dergelijke elementen zwijgt de bepaling volledig. Hij besluit dat hierdoor een reële wissing ontbreekt en dat in de praktijk profilering permanent wordt.

Voorts is er geen expliciete bewaartermijn voor backups en *disaster recovery*. Zonder aparte termijnen blijven gewiste gegevens feitelijk bestaan. Omdat het hier persoonsgebonden gegevens betreft, moeten volgens hem specifieke termijnen worden vastgelegd maar ook dit ontbreekt.

Hij merkt op dat de gegevens deels afkomstig zijn uit het CAP en dat de termijn niets vermeldt over de samenloop van gegevens en wie het tijdstip bepaalt. Er bestaat ook geen regeling voor synchronisatie tussen de Nationale Bank, de FOD Financiën en andere instanties. Indien de brongegevens worden gewist, dient ook de afgeleide kopie te worden verwijderd, hetgeen hij aanduidt als cascading deletion. Het gevolg is een dubbele, niet-gesynchroniseerde opslag en onnodige bewaring van gegevens.

Er wordt gesproken over de definitieve beëindiging van alle administratieve en gerechtelijke procedures, rechtsmiddelen en de integrale betaling. Hij merkt op dat dit in invorderingsdossiers vaak jaren na de verjaring van de aanslag gebeurt. Daardoor wordt de opslag van alle betrokken gegevens gekoppeld aan het langste traject, wat leidt tot overbewaring van irrelevante en ongebruikte data.

Precieze bewaartermijnen ontbreken waardoor de betrokkenen niet correct kunnen worden geïnformeerd over de duur van opslag en de criteria daarvoor. Volgens het lid wordt het recht op verwijdering van persoonsgegevens zoals voorzien in de AVG in de praktijk aldus denkbeeldig, aangezien er dagelijks nog procedures kunnen lopen en archivering op basis van artikel 89 van

qui résultent des traitements dans le *datawarehouse*, y compris les données dérivées telles que les scores, variables et labels. Un délai de conservation plus court n'est pas prévu pour, par exemple, les scores de risque qui sont, par définition, temporaires. Selon le membre, il n'existe aucun système d'expiration automatique des scores de risque, ni aucun mécanisme de désapprentissage du modèle (*model unlearning*) lorsque les données d'entraînement sont effacées. L'intervenant indique que les paramètres de modèle, qui ont été appris à partir de données à caractère personnel, demeurent des données à caractère personnel lorsqu'ils peuvent être reliés à une personne ou produire des biais. La disposition n'évoque absolument pas ces éléments. Le député en conclut qu'il ne s'agit pas d'un véritable effacement et que le profilage est permanent dans la pratique.

Par ailleurs, un délai de conservation n'est pas explicitement prévu pour les copies de sauvegarde (*backup*) ni pour le plan de reprise après sinistre (*disaster recovery*). En l'absence de délais distincts, les données effacées continuent en réalité d'exister. Comme il s'agit de données à caractère personnel, l'intervenant estime qu'il faudrait préciser des délais spécifiques, ce que ne prévoit pas le texte à l'examen.

Le membre relève que les données proviennent en partie du PCC et qu'aucune précision n'est donnée, en ce qui concerne le délai, sur le concours de plusieurs données ni sur le moment où le délai commence à courir. Il n'existe pas non plus de règle de synchronisation entre la Banque nationale, le SPF Finances et d'autres instances. Si les données sources sont effacées, il convient aussi de supprimer la copie dérivée selon un principe de suppression en cascade (*cascading deletion*), faute de quoi il en résultera un double stockage non synchronisé et une conservation inutile de données.

Il est question de la cessation définitive de toutes les procédures et recours administratifs et judiciaires, ainsi que du paiement intégral. Il fait observer que, dans les dossiers de recouvrement, tous ces éléments interviennent souvent plusieurs années après la prescription de l'imposition. Par conséquent, la conservation de toutes les données concernées est alignée sur le délai le plus long, ce qui entraîne une rétention excessive d'informations non pertinentes et inutilisées.

L'absence de précision sur les délais de conservation empêche d'informer correctement les personnes concernées sur la durée de stockage de leurs données et sur les critères applicables. Selon le membre, le droit à l'effacement des données à caractère personnel prévu par le RGPD devient ainsi purement théorique, puisque des procédures peuvent être engagées à tout

de AVG mogelijk blijft. Dit verhoogt volgens hem het risico op handhaving en vormt een probleem.

Het Hof van Justitie staat ook zeer kritisch tegenover structurele, preventieve en langdurige bewaring van bulkgegevens, zelfs met waarborgen. Een overkoepelende, proceduregedreven maximumtermijn die in de praktijk jaren of decennia kan worden, botst met de rechtsbescherming van burgers. Vooral wanneer gegevens voor profilering en datamining worden bewaard zonder concrete, individuele noodzaak ontstaat er een hoog risico op onverenigbaarheid met de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie.

Volgens de spreker ontbreken een aantal zaken in het tweede lid van de bepaling zoals een doelspecifieke, korte termijn voor gegevens. Hij stelt voor om te bepalen dat preselectie en risicoscores automatisch vervallen na 12 tot 24 maanden, tenzij dit leidt tot de opening van een individueel dossier. Onderzoeksdossiers zonder een vastgestelde inbreuk dienen binnen een X aantal jaren na afsluiting te worden gewist, dossiers met aanslag/sancties binnen een jaar na onherroepelijkheid. Een heldere koppeling met betrekking tot de betrokkenen ontbreekt eveneens. Het huidige artikel hanteert een veel te brede formulering door alle vorderingen die tot de bevoegdheid van de verwerkingsverantwoordelijke behoren in te sluiten. Hij stelt voor om dit te vervangen door een verwijzing naar de vorderingen die specifiek betrekking hebben op de betrokkenen en het betreffende dossier. Artikel 89 van de AVG moet worden geconcretiseerd. Hij vraagt dat er expliciet wordt gesproken over anonimiseren en pseudonimiseren, met vermelding van de doelen en de governance, waaronder onderzoeksstatistiek en ethische legal reviews. Voorts ontbreken model- en featuresbeheer, zoals verval van risicoscores en labels en een verbod op het gebruik van historische scores buiten het oorspronkelijke doel. Bij backups en replica's is er volgens hem een aparte, kortere termijn noodzakelijk, evenals een technische afdwinging. Ook moet de opslag onherroepelijk worden gekoppeld aan rechtskracht en niet aan de volledige betaling. Preselectie en analytische data moeten volgens het lid worden gescheiden van het juridisch dossier en dienen eigen, korte termijnen te hebben. Voorts dienen de betrokkenen ex-post te worden geïnformeerd over de beëindiging van de verwerking. Op de bewaartermijnen moet er een onafhankelijk toezicht plaatsvinden.

moment et que l'archivage reste possible sur la base de l'article 89 du RGPD. Cette situation accroît, selon lui, le risque de mesures de contrôle et représente un véritable problème.

La Cour de justice se montre également très critique à l'égard de la conservation structurelle, préventive et prolongée de données en masse, même assortie de garanties. Une durée maximale globale fondée sur la procédure — qui peut en pratique s'étendre sur plusieurs années, voire des décennies — entre en conflit avec la protection juridique des citoyens. Le risque d'incompatibilité avec les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne devient particulièrement élevé lorsque les données sont conservées à des fins de profilage et de *data mining* sans nécessité individuelle concrète.

Selon l'intervenant, plusieurs éléments font défaut dans l'alinéa 2 de la disposition, notamment un délai de conservation des données spécifique et limité en fonction de la finalité du traitement. Il propose de prévoir que la présélection et les scores de risque expirent automatiquement après 12 à 24 mois, sauf si cela conduit à l'ouverture d'un dossier individuel. Les dossiers d'enquête sans infraction constatée doivent être supprimés dans un délai déterminé après leur clôture, et les dossiers se soldant par une imposition ou une sanction doivent l'être un an après que la décision est devenue définitive. Un lien clair avec les personnes concernées fait également défaut. L'article actuel est formulé de manière trop large, en ce qu'il inclut toutes les actions qui relèvent de la compétence du responsable du traitement. Il propose de le remplacer par une référence aux actions se rapportant spécifiquement aux personnes concernées et au dossier correspondant. L'article 89 du RGPD doit être mis en œuvre de manière concrète. Il demande qu'il soit explicitement fait mention de l'anonymisation et de la pseudonymisation, en précisant les finalités et la gouvernance, ce qui inclut les statistiques de recherche et des examens juridiques et éthiques. En outre, la gestion des modèles et des variables fait défaut, comme en témoigne l'absence de durée de validité des scores de risque et des labels, et l'absence d'interdiction d'utiliser des scores historiques hors de la finalité initiale. Selon lui, les sauvegardes et les copies nécessitent un délai distinct et raccourci assorti d'un mécanisme technique garantissant son application. De plus, le stockage doit être irrévocablement lié à la force juridique et non au paiement intégral. Les données de présélection et d'analyse doivent être séparées du dossier juridique et faire l'objet de délais propres et limités. Les personnes concernées doivent être informées *ex post* de la cessation du traitement. Un contrôle indépendant doit être exercé sur les délais de conservation.

De heer Van Quickenborne stelt voor om het tweede lid aldus te amenderen:

“De bewaartermijn moet per verwerkingsdoel vooraf worden vastgesteld en publiek gemaakt.

Gegevens die uitsluitend worden verwerkt voor preselectie, risicoscoring of datamining, zonder individuele aanwijzingen, moeten binnen twaalf maanden worden gewist of onomkeerbaar geanonimiseerd, tenzij dit leidt tot de opening van een individueel dossier.

Gegevens in een individueel dossier zonder vastgestelde inbreuk dienen binnen drie jaar na afsluiting te worden gewist.

Gegevens in dossiers met een onherroepelijke beslissing worden binnen vijf jaar na onherroepelijkheid gewist.

Backups en logs volgen afzonderlijke beperkte termijnen.

Afwijkingen kunnen enkel met inachtneming van artikel 89 van de AVG en met passende waarborgen en voorafgaandelijke digital process impact assessment worden toegestaan.

De termijnen gelden per betrokken persoon en per dossier en worden niet verlengd door vorderingen die geen verband houden met de specifieke verwerking.”

De spreker bespreekt vervolgens het derde lid dat gaat over pseudonimisering waarbij de volgende vier stappen worden gehanteerd: eerst pseudonimisering via een zogenaamde anonieme sleutel, daarna integratie in het datawarehouse, vervolgens samenvoegen en tot slot analyse en profilering. Het gebruik van de term “anonieme sleutel” is evenwel verwarrend omdat in de AVG-terminologie deze notie niet wordt gebruikt. Hij herinnert eraan dat alle AVG-plichten, waaronder rechtmatigheid, doelbinding, minimale bewaring en de waarborgen van artikel 22 bij profilering, blijven gelden. Het gebruik van de term “anonieme sleutel” kan de indruk wekken van veiligheid maar verandert de juridische kwalificatie niet. Het kan later niet worden ingeroepen om strengere waarborgen te omzeilen. Hij benadrukt dat pseudonimisering en anonimisering juridisch verschillend zijn.

Ook het sleutelbeheer blijft onduidelijk: wie beheert de sleutel, is dat de verwerkingsverantwoordelijke of de verwerker? Waar bevindt de sleutel zich, is deze fysiek of logisch gescheiden van het datawarehouse? Hoe wordt

M. Van Quickenborne propose de remplacer l’alinéa 2 par ce qui suit:

“Le délai de conservation doit être fixé à l’avance pour chaque finalité de traitement et rendu public.

Les données traitées uniquement à des fins de présélection, de classification des risques ou de *data mining*, sans indices individuels, doivent être effacées ou rendues irréversiblement anonymes dans un délai de douze mois, sauf si cela conduit à l’ouverture d’un dossier individuel.

Les données contenues dans un dossier individuel sans infraction constatée doivent être effacées dans les trois ans de la clôture.

Les données des dossiers ayant fait l’objet d’une décision irrévocable doivent être effacées dans les cinq ans de la décision.

Les sauvegardes et les journaux (*logs*) suivent des délais limités distincts.

Les dérogations ne peuvent être autorisées que dans le respect de l’article 89 du RGPD, avec des garanties appropriées et après une analyse préalable de l’impact numérique (*digital process impact assessment*).

Les délais s’appliquent par personne concernée et par dossier, et ne sont pas prolongés par des actions sans lien avec le traitement spécifique.”

L’intervenant aborde ensuite l’alinéa 3, consacré à la pseudonymisation, et décrit quatre étapes: d’abord la pseudonymisation au moyen d’une “clé anonyme”, puis l’intégration dans la *datawarehouse*, ensuite l’agrégation des données, et enfin l’analyse et le profilage. L’utilisation du terme “clé anonyme” prête toutefois à confusion, car cette notion n’apparaît pas dans la terminologie du RGPD. Il rappelle que toutes les obligations du RGPD, notamment la licéité, la limitation des finalités, la minimisation des données et les garanties de l’article 22 en matière de profilage, restent applicables. De plus, l’emploi du terme “clé anonyme” peut donner une impression de sécurité, mais ne modifie en rien la qualification juridique et ne peut pas être invoqué ultérieurement pour contourner des garanties plus strictes. Le membre souligne que la pseudonymisation et l’anonymisation sont deux notions juridiquement distinctes.

La gestion des clés reste également floue: qui s’en charge, le responsable du traitement ou le sous-traitant? Où se trouve la clé, est-elle physiquement ou logiquement séparée de la *datawarehouse*? Comment l’accès est-il

toegang verleend? Hoe vaak worden sleutels geroteerd? Wat bij een datalek? Wat met een cascade deletion?

Over de deterministische koppeling. Voor datamatching zullen vrijwel zeker deterministische pseudoniemen worden gebruikt; anders is samenvoegen onmogelijk. Dit betekent cross dataset tracking over tijd, zelfs als de naam verborgen is. Met voldoende quasi-identifiers zoals postcode, leeftijd, activiteit, transactiepatronen kan een persoon opnieuw worden geïdentificeerd zonder dat de sleutel nodig is. Gevolg: een hoge re-identificatiekans en profilering by design.

De pseudonimisering dient overeenkomstig de tekst voorafgaandelijk aan de integratie in het datawarehouse te gebeuren. Maar waar gebeurt de pseudonimisering precies? Bij de bron, bijvoorbeeld de Nationale Bank of na extractie bij de FOD Financiën? Als het bij de FOD gebeurt, passeren de ruwe persoonsgegevens toch de pipeline en blijft er een risico. Als het bij de bron gebeurt, is dat beter voor dataminimalisatie maar zijn strikte mandaten en onafhankelijke sleutelbewaring vereist. Hierover vermeldt de tekst evenwel niets.

Wat de beslissing tot kijken betreft. Deze passage bepaalt de technische voorwaarden voor het koppelen en scoren. Nergens is vastgelegd dat de overgang van token naar identiteit vooraf door een mens moet worden gevalideerd met een motivering. De spreker herinnert eraan dat bij profilering evenwel artikel 22 van de AVG—recht op menselijke tussenkomst en uitlegbaarheid—relevant is maar dat dit hier volledig ontbreekt. Het risico is dat depseudonimisering automatisch gebeurt, enkel op basis van modelscoren. Depseudonimisering blijft immers verwerking van persoonsgegevens maar er komt geen menselijke tussenkomst aan te pas.

Het systeem laat ook toe dat datasets worden samengevoegd. Er is geen doelbeperking. Welke combinaties zijn toegestaan? Welke niet?

Daarnaast stelt de spreker het ontbreken van de volgende gegevens vast:

— Geen RIA of DPIA;

accordé? À quelle fréquence les clés sont-elles renouvelées? Que se passe-t-il en cas de fuite de données? Qu'en est-il de la suppression en cascade?

E ce qui concerne l'appariement, des pseudonymes déterministes sont très probablement utilisés pour le *datamatching*, sans quoi l'agrégation serait impossible. Cette technique permet un suivi croisé des individus dans le temps à travers plusieurs bases de données (*cross dataset tracking*), même si leur nom est masqué. Avec un nombre suffisant de quasi-identifiants tels que le code postal, l'âge, l'activité ou les schémas de transactions, une personne peut être à nouveau repérée sans recourir à la clé, ce qui entraîne un risque élevé de réidentification et de profilage dès la conception.

Selon le texte, la pseudonymisation doit être effectuée avant l'intégration dans la *datawarehouse*. La question se pose alors de savoir où elle a lieu exactement: à la source, par exemple à la Banque nationale, ou après extraction par le SPF Finances? Si elle se fait au SPF, les données personnelles brutes traversent le pipeline, ce qui maintient un risque. Si elle se fait à la source, cela favorise la minimisation des données, mais nécessite des mandats stricts et une gestion indépendante des clés. Le texte ne précise toutefois rien à ce sujet.

Pour ce qui est de la décision de consultation, le passage concerné fixe les conditions techniques pour le couplage des données et l'évaluation des risques (score de risque). Il n'est en revanche précisé nulle part que la dépseudonymisation (identification sur la base du *token*) devra être validée au préalable par un être humain en motivant les raisons de cette action. L'intervenant rappelle qu'en cas de profilage, l'article 22 du RGPD – droit d'obtenir une intervention humaine et des explications – est toutefois applicable, mais qu'il est totalement absent du projet de loi à l'examen. Le risque est que la dépseudonymisation se fasse automatiquement, sur la seule base du score attribué au risque concerné. En effet, la dépseudonymisation reste un traitement de données à caractère personnel qui ne nécessite pas d'intervention humaine.

Le système permettra également de fusionner des ensembles de données. Il ne prévoit pas de limitation des finalités. Quelles combinaisons de données seront autorisées et, inversement, quelles combinaisons seront interdites?

L'intervenant poursuit en déplorant l'absence des éléments suivants:

— Pas de règles relatives à l'intelligence artificielle, ni d'analyse d'impact relative à la protection des données;

— Geen feature governance: welke kenmerken mogen in modellen en welke zijn verboden proxy's? Aldus wordt de proportionaliteit moeilijk toetsbaar.

— Geen technische specificaties: normaal staat in de wet dat de Koning bij besluit de specificaties nader bepaalt. In voorkomend geval ontbreekt elk uitvoeringsbesluit.

Het lid stelt voorts vast dat in de praktijk de ter bespreking voorliggende bepalingen de door de AVG bepaalde rechten (artikelen 13, 14, 15, 21 en 22) uithollen. De brede pseudonimisering en koppeling maken het bijna onmogelijk om uit te leggen welke gegevens in welke analyse zijn gebruikt. Zonder modelcards en beslislogboeken is uitlegbaarheid een illusie wat leidt tot hoge handavingsrisico's. Europese rechtspraak toont ook aan dat systemen die criteria aanpassen zonder menselijke controle onverenigbaar zijn met het EU-recht.

Terugkomend op de term “anonieme sleutel” is de spreker van oordeel dat het eerder aangewezen is om de term “pseudonimisatiesleutel” te gebruiken. Deze moet, onafhankelijk van de verwerkingsomgeving, afzonderlijk worden bewaard en alleen toegankelijk zijn onder vooraf gedocumenteerde, goedgekeurde procedures met onveranderbare logging. Essentiële waarborgen die nodig zijn om dit verdedigbaar te maken, zijn onder meer een heldere key governance, zijnde een onafhankelijke sleutelbewaring, bijvoorbeeld bij de Nationale Bank of een derde trustparty. Ook dient er een verbod te zijn op operationele toegang tot mappingtabellen in analytische omgevingen. Er moet tokenisatie zijn bij overdracht naar de FOD Financiën. Er moet een wettelijk register van toegestane koppelingen zijn. Depseudonimisering kan enkel na menselijke beslissing: gemotiveerd en gebaseerd op vooraf wettelijk vastgelegde criteria met een verplicht ex-post notificatie aan de betrokkenen. Tevens dient er een verbod te zijn op zelflerende drift zonder menselijke review. Er moet ook een lijst van toegestane modellen en modelcards voorhanden zijn, alsook een expliciet verbod op verboden proxy's (bijv. postcode als een indirecte socio-demografische proxy). Inzake de uitlegbaarheid dienen er beslislogs en een externe audittoegang te zijn.

— Pas de gouvernance des fonctionnalités (*feature governance*): quelles caractéristiques seront autorisées dans les modèles utilisés et quels *proxys* seront interdits? Il sera ainsi difficile de contrôler la proportionnalité;

— Pas de spécifications techniques: la loi prévoit en principe que le Roi fixera ultérieurement les spécifications par arrêté d'exécution. Or, dans le texte à l'examen, aucun arrêté d'exécution n'est prévu.

Par ailleurs, le membre constate que les dispositions à l'examen éroderont en pratique les droits prévus par le RGPD (articles 13, 14, 15, 21 et 22). En raison de la pseudonymisation et du couplage à grande échelle, il sera pratiquement impossible d'expliquer quelles données ont été utilisées dans telle ou telle analyse. Sans cartographie des modèles utilisés et sans journalisation des décisions, le droit d'obtenir des explications ne sera qu'illusion, ce qui entraînera des risques élevés pour l'application de la loi. Il ressort également de la jurisprudence européenne que les systèmes qui modifient les critères sans contrôle humain sont incompatibles avec le droit de l'Union européenne.

L'intervenant souhaite revenir ensuite sur la notion de “clé anonyme”. Il estime qu'il serait préférable d'employer la notion de “clé de pseudonymisation”, dès lors que celle-ci devra être conservée séparément – en dehors de l'environnement de traitement – et ne devra être accessible que dans le cadre de procédures préalablement documentées, approuvées et soumises à un système de journalisation immuable. Un tel système n'est défendable que s'il repose sur des garanties essentielles telles que des règles de gestion claires des clés (*key governance*) prévoyant notamment un stockage indépendant des clés, par exemple auprès de la Banque nationale ou d'un tiers de confiance. Il conviendra également d'interdire l'accès opérationnel aux tableaux de correspondance dans les environnements analytiques et de procéder à la tokenisation lors du transfert des données vers le SPF Finances. Un registre légal des couplages autorisés devra également être instauré. La dépersonnalisation ne sera autorisée que moyennant une décision humaine: elle devra être motivée et reposer sur des critères préalablement fixés par la loi, et les personnes concernées devront obligatoirement en être informées *a posteriori*. Il conviendra également d'interdire les systèmes d'apprentissage automatique sans contrôle humain, d'établir la liste des modèles et des cartographies de modèles autorisés, et d'identifier explicitement les *proxys* interdits (par exemple, le code postal comme *proxy* sociodémographique indirect). En ce qui concerne le droit d'obtenir des explications, il conviendra de prévoir des journaux de décisions auxquels les audits externes pourront avoir accès.

Concreet betekent dit dat het derde lid dient te worden herschreven in de zin dat de persoonsgegevens, zoals bedoeld in het eerste lid, voorafgaand aan elke overdracht naar het voormeld datawarehouse worden gepseudonimiseerd met een pseudonimisatiesleutel. De pseudonimisatiesleutel en de mappingtabellen worden afzonderlijk bewaard onder onafhankelijk beheer en zijn niet toegankelijk voor de verwerkingsomgeving. Depseudonimisering mag uitsluitend plaatsvinden na een menselijke, voorafgaande beslissing, gebaseerd op wettelijk vastgelegde criteria, met motivering en onveranderbare logging. Samenvoeging met andere datasets en analyses is alleen toegestaan voor uitdrukkelijk bepaalde doeleinden die vooraf zijn onderworpen aan een gegevensbeschermingseffectbeoordeling waarvan een publiek samenvattend verslag beschikbaar is. De heer van Quickenborne kondigt aan dat hij dit tekstvoorstel als amendement zal indienen.

Het vierde lid is volgens de spreker op juridisch vlak de trigger voor depseudonimisering in het kader van *money control*. Het is de fase waarin een pseudoniem profiel wordt terugvertaald naar de werkelijke identiteit (naam, registratienummer). De logica is dat de fiscus eerst de gepseudonimiseerde gegevens verwerkt; pas bij een op basis van vooraf bepaalde risicofactoren vastgesteld risico mag de administratie de sleutel gebruiken om de persoon te identificeren. Alhoewel dit op het eerste gezicht op een waarborg lijkt, creëert het in werkelijkheid een quasi-onbeperkte bevoegdheid: de termen zijn immers vaag, elastisch en intern bepaalbaar.

Er is voorts ook geen wettelijke definitie of exhaustieve lijst van risicofactoren, noch wie deze vaststelt of valideert, voorhanden. De FOD Financiën kan deze risicofactoren intern bepalen, via algoritmische criteria, beslissingsbomen of machine learning. De kern van de controlebevoegdheid ligt dus niet in de wet maar in een intern model buiten democratische toetsing. Volgens de rechtspraak van het Hof van Justitie moeten wetten die persoonsgegevens verwerken of koppelen duidelijk en voorspelbaar zijn, zodat burgers weten wanneer zij kunnen worden geraakt. Vooraf vastgestelde risicofactoren ontbreken hier evenwel. De bevoegdheid wordt feitelijk gedelegeerd aan een algoritme en maakt aldus een schending uit van het legaliteitsbeginsel, artikel 22 van de Grondwet en artikel 8 van het EVRM. Als *money control* machine learning gebruikt, worden risicofactoren dynamisch aangepast en zijn ze per definitie niet vooraf bepaald. Het Hof van Justitie heeft expliciet gesteld dat systemen met zelflerende technologie onverenigbaar zijn met het vereiste van vooraf bepaalde criteria, omdat ze zonder menselijke tussenkomst een weging wijzigen.

Concrètement, cela signifie que l'alinéa 3 doit être reformulé de manière à ce que les données à caractère personnel visées à l'alinéa 1^{er} soient pseudonymisées au moyen d'une clé de pseudonymisation avant tout transfert vers le *data warehouse* précité. La clé de pseudonymisation et les tableaux de correspondance seront conservés séparément sous gestion indépendante et ne seront pas accessibles dans l'environnement de traitement. La dépseudonymisation ne sera autorisée que moyennant une décision humaine préalable, fondée sur des critères préalablement fixés par la loi, motivée et dûment journalisée. Toute fusion avec d'autres ensembles de données et toute analyse ne seront autorisées qu'à des fins expressément déterminées, préalablement soumises à une analyse d'impact relative à la protection des données, dont le rapport récapitulatif sera rendu public. M. Van Quickenborne annonce qu'il présentera une proposition de texte en ce sens sous la forme d'un amendement.

L'intervenant estime que l'alinéa 4 de l'amendement à l'examen fournira le fondement juridique de la dépseudonymisation dans le cadre du *money control*. Il s'agit de la phase au cours de laquelle l'identité réelle (nom, numéro d'enregistrement) d'une personne est extraite d'un profil pseudonymisé. La logique veut que le fisc utilise d'abord les données pseudonymisées à des fins de traitement; ce n'est qu'en cas de risque identifié sur la base de facteurs de risque prédéterminés que l'administration pourra utiliser la clé pour identifier la personne concernée. Bien qu'à première vue, cette disposition semble constituer une garantie, elle accorde en réalité un pouvoir quasi illimité: ses termes sont en effet vagues, élastiques et laissés à l'appréciation en interne.

Le texte à l'examen ne prévoit par ailleurs aucune définition légale ni de liste exhaustive des facteurs de risque. Il ne précise pas non plus qui sera chargé de les déterminer ou de les valider. Le SPF Finances pourra déterminer ces facteurs de risque en interne, au moyen de critères algorithmiques, d'arbres de décision ou de techniques d'apprentissage automatique. Les éléments essentiels de ce pouvoir de contrôle ne seront donc pas inscrits dans la loi, mais fixés ultérieurement dans un modèle interne échappant à tout contrôle démocratique. Selon la jurisprudence de la Cour de justice, les lois traitant ou couplant des données à caractère personnel doivent être claires et prévisibles pour permettre aux citoyens de savoir quand ils peuvent en subir les effets. Or, le texte à l'examen ne contenant pas de facteurs de risque préalablement fixés, leur identification sera en réalité confiée à un algorithme, ce qui constitue une violation du principe de légalité, de l'article 22 de la Constitution et de l'article 8 de la CEDH. Si le *money control* repose sur l'apprentissage automatique, les facteurs de risque seront ajustés de manière dynamique et

Verwijzend naar de parlementaire vraag (nr. 75) van 11 februari 2022 inzake de toeslagenaffaire van de heer Steven Matheï aan de toenmalige minister van Financiën Van Peteghem heeft deze laatste gesteld dat de wet vooraf vastgestelde factoren vereist. Maar de praktijk werkt met adaptieve modellen, wat dus intrinsiek incoherent is. De spreker stipt aan dat het hier niet gaat om vastgestelde inbreuken of concrete aanwijzingen maar om een risico dat iemand mogelijk een misdrijf kan plegen. Dat is dus een preventieve logica. De fiscale administratie zou dus kunnen handelen op basis van een vermoeden, nog voordat een overtreding heeft plaatsgevonden. Dit is predictive policing in fiscale vorm: preventieve controle op basis van mogelijke, nog niet gepleegde inbreuken. Het is het verschuiven van reactief toezicht naar preventief toezicht. Het vermoeden van onschuld wordt aldus ingeruild voor het vermoeden van schuld. Bovendien wordt in de tekst van het vierde lid ook geen onderscheid gemaakt tussen een klein risico, zoals een kleine afwijking, en een groot risico, zoals systemische fraude. Een klein risico, zoals een afwijkende aangifte, wordt op dezelfde manier behandeld als een groot risico, bijvoorbeeld systematische of georganiseerde fraude. Elke risicoscore kan dus volstaan voor het onthullen van de identiteit. Er is geen verplichting tot menselijke bevestiging of juridische toetsing bij deze depseudonimisering.

Het lid merkt op dat door sommigen wordt verwezen naar “georganiseerde fraude” terwijl de wettekst het daadwerkelijk heeft over “een inbreuk op een wet of een reglementering waarvan de toepassing behoort tot de opdrachten van de Federale Overheidsdienst Financiën”. Met andere woorden: elke inbreuk op de fiscaliteit, inclusief circulaires, koninklijke besluiten, ministeriële besluiten en honderden domeinen, valt hieronder. Concreet betekent dit dat elk afwijkend patroon, zelfs een administratieve afwijking, kan worden gebruikt om *money control* toe te passen. Het gaat hier dus niet specifiek over fiscale fraude – het woord “fraude” staat zelfs niet in de tekst – noch over onregelmatigheden met fraudeleus oogmerk. Een te laat ingediende aangifte of een kleine vergissing kan al als “inbreuk” gelden. Dit is wat men een kanon op een mug zou kunnen noemen: disproportioneel en zwaar voor relatief kleine overtredingen. Aldus wordt in

ne seront, par définition, pas prédéterminés. La Cour de justice a explicitement indiqué que les systèmes recourant aux technologies d'apprentissage automatique sont incompatibles avec l'exigence de critères prédéterminés, au motif qu'ils altèrent une conclusion sans intervention humaine. En réponse à la question parlementaire (n° 75) concernant l'affaire des allocations familiales aux Pays-Bas, posée le 11 février 2022 par M. Steven Matheï à M. Van Peteghem, alors ministre des Finances, ce dernier a indiqué que la loi exige des facteurs prédéterminés. Or, la pratique reposera en l'occurrence sur des modèles adaptatifs, ce qui sera donc intrinsèquement incohérent. L'intervenant souligne que le système ne s'appuiera pas sur des infractions constatées, ni sur des indices concrets, mais sur le risque que quelqu'un puisse commettre une infraction. Il s'agit donc d'une logique préventive. L'administration fiscale pourrait donc agir sur la base d'une présomption, avant même qu'une infraction n'ait été commise. Les principes de la police prédictive (*predictive policing*) seront appliqués à la fiscalité: des contrôles seront menés préventivement et cibleront des infractions potentielles, mais qui n'ont pas encore été commises. Autrement dit, on passera d'un contrôle réactif à un contrôle préventif. La présomption d'innocence cédera ainsi la place à la présomption de culpabilité. Qui plus est, le texte de l'alinéa 4 n'opère aucune distinction entre un risque faible, par exemple une dérogation mineure à la loi, et un risque élevé, comme une fraude systémique. Ainsi, un risque faible, par exemple une déclaration irrégulière, sera traité de la même manière qu'un risque élevé, par exemple une fraude systématique ou organisée. Le risque, quel que soit son score, pourra donc suffire pour révéler l'identité d'une personne. Cette depseudonymisation ne sera soumise à aucune obligation de confirmation par un être humain, ni de contrôle juridique.

Le membre fait observer que certains font référence à une “fraude organisée”, alors que le texte de loi parle en réalité d’“un risque de commission d’une infraction à une loi ou à une réglementation dont l’application relève des missions du Service public fédéral Finances”. Autrement dit, le texte sera applicable à toute infraction aux règles fiscales, y compris les circulaires, les arrêtés royaux, les arrêtés ministériels et des centaines d’autres domaines. Concrètement, cela signifie que toute méconnaissance d’une règle, même administrative, pourra donner lieu à l’application du *money control*. Le texte ne vise donc pas spécifiquement la fraude fiscale – le mot “fraude” n’apparaît même pas dans le texte – ou les irrégularités commises dans une intention frauduleuse. Une déclaration déposée trop tardivement ou une petite erreur pourront déjà être considérées comme une “infraction”. C’est ce qu’on pourrait appeler tuer une mouche avec

strijd met de EU-wetgeving het vermoeden van goeder trouw volledig ondergraven.

Daarnaast stelt de tekst dat een depseudonimisering kan plaatsvinden, zonder procedurele voorwaarden. Het is evenwel onduidelijk wie beslist wanneer de drempel is bereikt. Is dat een geautomatiseerde trigger of is er een menselijke validatie? Is er controle door een DPO of een onafhankelijke auditor? Er is geen verplichting tot motivering, logging of schriftelijk verslag, geen audit-trail, geen melding aan de Gegevensbeschermingsautoriteit en geen kennisgeving aan de betrokkenen – terwijl de artikelen 13, 14 en 22 van de AVG dit expliciet voorschrijven. Zonder toezicht kan elk model, en zeker AI, duizenden onterechte risico's genereren wat kan leiden tot massale depseudonimisering van gegevens, vergelijkbaar met wat er in de toeslagenaffaire in Nederland is gebeurd.

De juridische toetsing aan de EU-rechtspraak maakt dit nog problematischer. In het arrest *Digital Rights Ireland* (C-293/12) heeft het Europees Hof van Justitie geoordeeld dat de algemene bewaring en analyse van communicatiegegevens zonder concrete link met ernstige criminaliteit onverenigbaar is met het EU-recht. Hier gebeurt iets soortgelijks: algemene risicobeoordeling leidt tot depseudonimisering zonder concrete, individuele aanleiding. In het arrest *Tele2 Sverige* (C-203/15) stelt het Hof dat toegang tot data alleen is toegestaan voor specifieke gevallen en onder voorafgaande toetsing door een onafhankelijke instantie. In de huidige tekst ontbreekt zowel die onafhankelijke toetsing als een concrete afbakening van de gevallen. In het arrest *La Quadrature du Net* (C-511/18) sluit het Hof uit dat preventieve, permanente risicobeoordeling van burgers proportioneel is. De ter bespreking voorliggende tekst introduceert echter volgens het lid een risicomodel dat preventief depseudonimiseert en strijdig is met de EU-richtlijnen en het proportionaliteitsbeginsel. In de PNR-zaak wordt duidelijk gesteld dat vooraf bepaalde criteria menselijk moeten worden vastgesteld en dat zelflerende profilering zonder menselijke controle in strijd is met het Handvest van de grondrechten van de Europese Unie. De heer Van Quickenborne kan evenwel alleen maar vaststellen dat de voorgestelde bepaling exact dezelfde formulering handhaaft als de tekst die door het Europees Hof werd vernietigd. Het fundamenteel probleem gaat evenwel nog verder. De cruciale drempel voor toezicht – namelijk wanneer de identiteit kan worden onthuld – wordt niet bepaald door de wet of een rechter maar door een intern risicomodel. Het Parlement krijgt geen inzage in de criteria of de foutenmarge en de betrokken burgers

un canon. Il s'agit d'une réaction disproportionnée et sévère à des manquements relativement mineurs. Ce procédé sape complètement la présomption de bonne foi, en violation de la législation européenne.

En outre, le texte prévoit qu'une depseudonymisation pourra avoir lieu sans conditions procédurales. Cependant, il n'est pas indiqué clairement qui décidera à quel moment le seuil est atteint. Est-il question d'un déclencheur automatisé ou d'une validation humaine? Y aura-t-il un contrôle par un DPO ou un auditeur indépendant? Le texte ne prévoit aucune obligation de motivation, de logging ou de rapport écrit, aucune piste d'audit, aucune notification à l'Autorité de protection des données et aucune notification aux personnes concernées, alors que les articles 13, 14 et 22 du RGPD le prescrivent explicitement. Sans contrôle, tout modèle, et certainement l'IA, est susceptible de générer des milliers de risques injustifiés pouvant conduire à une depseudonymisation massive des données, comparable à ce qui s'est produit dans l'affaire des allocations aux Pays-Bas.

Le contrôle juridique au regard de la jurisprudence de l'UE rend ce point encore plus problématique. Dans l'arrêt *Digital Rights Ireland* (C-293/12), la Cour de justice de l'Union européenne a considéré que la conservation et l'analyse généralisées de données de communication sans lien concret avec des formes graves de criminalité sont incompatibles avec le droit européen. On assiste en l'occurrence à une situation similaire: l'évaluation globale des risques conduit à une depseudonymisation sans motif concret et individuel. Dans l'arrêt *Tele2 Sverige* (C-203/15), la Cour a souligné que l'accès aux données n'est autorisé que dans des cas spécifiques et est soumis à un contrôle préalable exercé par une instance indépendante. Le texte actuel ne prévoit ni contrôle indépendant, ni délimitation concrète des cas. Dans l'arrêt *La Quadrature du Net* (C-511/18), la Cour a exclu que l'évaluation préventive et permanente des risques présentés par les citoyens soit proportionnée. Or, selon le membre, le texte à l'examen introduit un modèle de risque qui depseudonymise de manière préventive et qui est contraire aux directives de l'UE et au principe de proportionnalité. Dans l'affaire PNR, il a clairement été souligné que les critères prédéfinis doivent être déterminés par des êtres humains et que le profilage autodidacte sans contrôle humain est contraire à la Charte des droits fondamentaux de l'Union européenne. M. Van Quickenborne ne peut toutefois que constater que la disposition proposée reprend exactement la même formulation que le texte annulé par la Cour européenne. Mais le problème fondamental excède ce seul aspect. Le seuil crucial pour le contrôle – à savoir le moment où l'identité peut être révélée – n'est pas déterminé par la loi ou par un juge, mais par un modèle de risque interne.

hebben geen mogelijkheid om een risicoscore aan te vechten. Volledig buiten elke democratische toetsing vindt aldus een ingrijpende machtsverschuiving van een publieke naar een algoritmische controle plaats.

Teneinde dit te herstellen en de tekst te verbeteren, doet het lid enkele suggesties. De wet moet concreet en limitatief bepalen welke criteria een depseudonimisering rechtvaardigen. Er dient in de wettekst zelf te worden voorzien in een verplichte menselijke validatie. Depseudonimisering mag pas plaatsvinden na beoordeling door ten minste twee ambtenaren via een gemotiveerd verslag of na controle door de DPO met melding aan een onafhankelijke toezichthouder zoals de Gegevensbeschermingsautoriteit. Een verbod op geautomatiseerde depseudonimisering moet worden ingeschreven. Elke stap moet gemotiveerd en onder toezicht plaatsvinden.

Het vierde lid van de nieuwe paragraaf 3 van artikel 5 van de wet van 3 augustus 2012 stelt dat er duidelijkheid moet zijn over de risicofactoren maar in werkelijkheid stelt de spreker vast dat er geen lijst voorhanden is. Alles wordt intern bepaald. Inzake noodzaak en proportionaliteit wordt een preventieve logica en geen concrete verdenking gehanteerd. Er wordt uitgegaan van het risico dat een regel wordt overtreden. In strijd met artikel 22 van de AVG wordt een menselijke tussenkomst niet ingeschreven. Ook een onafhankelijk toezicht en een democratische controle ontbreken. Het is vanzelfsprekend te verregaand dat alle domein van financiën onder het toepassingsgebied vallen. De voorgestelde regel is ook strijdig met de eerder vermelde EU-rechtspraak. Zonder de inschrijving van de eerder vermelde basisvoorwaarden is het vierde lid een passage die *money control* verandert van een data-analyse instrument naar een permanent, fiscaal surveillance systeem. Het algoritme beslist wanneer de “sluier” valt en burgers opnieuw met naam en identiteit worden geïdentificeerd.

Het vijfde lid voegt daarbovenop een automatische activeringsclausule toe: “Indien een depseudonimisatie plaats heeft, zal vervolgens aan de bevoegde controledienst worden gevraagd om een controle van het geselecteerde dossier uit te voeren.” Het wordt dus een automatisch proces. Zodra het algoritme een score boven een bepaalde drempel genereert, wordt de identiteit automatisch ontsloten en het dossier doorgestuurd naar de controledienst. De wet specificeert niet wie tot deze depseudonimisering beslist: een ambtenaar of het algoritme? In combinatie met het vierde lid wordt aldus een quasi-automatische depseudonimisering zonder menselijke toetsing gecreëerd.

Le Parlement n’a pas accès aux critères ni à la marge d’erreur, et les citoyens concernés n’ont pas la possibilité de contester un score de risque. C’est ainsi qu’en l’absence de tout contrôle démocratique, un transfert de pouvoir radical s’opère, passant d’un contrôle public à un contrôle algorithmique.

Afin de remédier à cette situation et d’améliorer le texte, le membre formule quelques suggestions. La loi doit définir de manière concrète et limitative les critères justifiant une dépseudonymisation. Le texte légal lui-même doit prévoir une validation humaine obligatoire. La dépseudonymisation ne peut avoir lieu qu’après évaluation par au moins deux fonctionnaires au moyen d’un rapport motivé ou après contrôle par le DPO avec notification à une autorité de contrôle indépendante telle que l’Autorité de protection des données. Une interdiction de la dépseudonymisation automatisée doit être prévue. Chaque étape doit être motivée et effectuée sous contrôle.

L’alinéa 4 du nouveau paragraphe 3 de l’article 5 de la loi du 3 août 2012 prévoit que les indicateurs de risque doivent être clairement définis, mais en réalité, l’intervenant constate qu’il n’existe aucune liste. Tout sera déterminé en interne. En matière de nécessité et de proportionnalité, on appliquera une logique préventive et non une suspicion concrète. On se basera sur le risque qu’une règle soit enfreinte. Aucune intervention humaine n’est prévue, ce qui est contraire à l’article 22 du RGPD. Il n’y aura pas non plus de contrôle indépendant ni de contrôle démocratique. Le fait que tous les domaines financiers relèvent du champ d’application des mesures à l’examen est évidemment excessif. La règle proposée est également contraire à la jurisprudence de l’UE mentionnée précédemment. Sans l’inscription des conditions de base susmentionnées, l’alinéa 4 est un passage qui transformera l’outil d’analyse de données qu’est *money control* en un système de surveillance fiscale permanent. L’algorithme décidera du moment où le “voile” sera levé et où les citoyens seront identifiés par leur nom et leur identité.

L’alinéa 5 ajoute une clause d’activation automatique: “Si une dépseudonymisation est réalisée, il sera alors demandé au service de contrôle compétent d’effectuer une vérification du dossier sélectionné”. Il s’agira donc d’un processus automatique. Dès que l’algorithme générera un score supérieur à un certain seuil, l’identité sera automatiquement dévoilée et le dossier sera transmis au service de contrôle. La loi ne précise pas qui décidera de cette dépseudonymisation: un fonctionnaire ou l’algorithme? En combinaison avec l’alinéa 4, on obtiendra donc une dépseudonymisation quasi automatique sans contrôle humain.

Volgens artikel 22 van de AVG is dit problematisch: de betrokken persoon mag niet worden onderworpen aan een uitsluitend geautomatiseerde besluitvorming die rechtsgevolgen heeft. In voorkomend geval ontbreekt elke garantie dat een menselijke beoordelaar de uiteindelijke beslissing kan wijzigen. De ambtenaar voert enkel uit zonder echte beoordelingsmacht. Dit terwijl de Europese EDPB benadrukt dat een menselijke tussenkomst daadwerkelijk de mogelijkheid moet bieden om het resultaat te wijzigen en niet louter formeel mag zijn. Dat is hier volgens het lid duidelijk niet het geval. De door de spreker geraadpleegde experts zijn dan ook eenstemmig van oordeel dat de tekst onzorgvuldig is opgesteld.

De heer Van Quickenborne bespreekt vervolgens het vijfde lid van het nieuwe artikel 95/3 dat werd ingevoegd door amendement nr. 16 (DOC 56 0963/005) in eerste lezing (DOC 56 0963/020). In die bepaling staat volgende zin “aan de bevoegde controledienst worden gevraagd”, maar nergens in het lid wordt verduidelijkt over welke dienst het gaat. Betreft het de FOD Financiën? Wie bepaalt welke dienst bevoegd wordt? De wet geeft hierover geen uitsluitsel.

De spreker concludeert dat de selectie voortaan centraal wordt aangestuurd vanuit de data-administratie. Dat houdt in dat de data-afdeling niet langer enkel een analytische, maar vooral ook een operationele en beslissende rol krijgt. Het commissielid stelt vast dat een team dat hoofdzakelijk bestaat uit data-analisten, dus niet uit fiscale ambtenaren, indirect zal bepalen waar het fiscaal opsporingsapparaat zijn aandacht op richt.

Bovendien ontbreken er volgens de heer Van Quickenborne enkele cruciale elementen in het lid. Zo ontbreekt vooreerst een motiveringsplicht. Wanneer een dossier via datamining wordt geselecteerd, ontvangt de belastingplichtige geen enkele kennisgeving. Hij beschikt bovendien niet over een intern beroep en kan geen bezwaar indienen tegen de selectie. De burger weet dus niet dat hij is geselecteerd, evenmin waarom dat is gebeurd, noch op basis van welke criteria dit is gebeurd. Volgens het lid vormt deze werkwijze een manifeste schending van de artikelen 13 tot en met 15 van de GDPR inzake transparantie, evenals van artikel 22, dat bescherming biedt tegen uitsluitend geautomatiseerde besluitvorming.

Daarnaast maakt de tekst, doordat de motiveringsplicht ontbreekt, geen onderscheid tussen een lichte verificatie en een volledig onderzoek. Een lichte verificatie betekent dat bijkomende informatie wordt opgevraagd; een volledig onderzoek kan daarentegen leiden tot

Ce point pose problème au regard de l'article 22 du RGPD: la personne concernée ne peut être soumise à une décision exclusivement automatisée ayant des conséquences juridiques. Il n'existe aucune garantie qu'un évaluateur humain puisse modifier la décision finale le cas échéant. Le fonctionnaire se bornera à un rôle d'exécutant sans véritable pouvoir d'appréciation. Or, l'EDPB européen souligne qu'une intervention humaine doit réellement permettre de modifier le résultat et ne peut être purement formelle. Selon l'intervenant, ce n'est manifestement pas le cas en l'occurrence. Les experts consultés par l'intervenant sont unanimes sur le fait que le texte a été rédigé avec peu de soin.

M. Van Quickenborne évoque ensuite l'alinéa 5 du nouvel article 95/3 inséré par l'amendement n° 16 (DOC 56 0963/005) en première lecture (DOC 56 0963/020). Cette disposition contient la phrase suivante: “il sera alors demandé au service de contrôle compétent”, mais cet alinéa ne précise nullement de quel service il s'agit. S'agit-il du SPF Finances? Qui déterminera le service compétent? La loi ne donne pas de réponse définitive à cette question.

L'intervenant en conclut que la sélection sera dorénavant pilotée de manière centralisée à partir de l'administration des données. Cela signifie que le service chargé des données n'aura plus seulement un rôle analytique, mais jouera aussi et surtout un rôle opérationnel et décisionnel. Le membre observe que ce sera une équipe composée principalement d'analystes de données, et donc pas de fonctionnaires du fisc, qui déterminera indirectement les domaines sur lesquels les services d'enquête fiscale se concentreront.

De plus, selon M. Van Quickenborne, certains éléments cruciaux font défaut dans l'alinéa précité. Il mentionne d'abord l'absence d'obligation de motivation. Lorsqu'un dossier sera sélectionné par le biais du *data mining*, le contribuable ne recevra aucune notification. Qui plus est, ce dernier ne disposera pas d'un recours interne et il ne pourra introduire aucune réclamation contre la sélection. Le citoyen ne saura donc pas pourquoi il a été sélectionné ni sur la base de quels critères. Le membre estime que cette procédure constituera une violation manifeste des articles 13 à 15 du RGPD en matière de transparence, ainsi que de son article 22, qui protège contre la prise de décision exclusivement automatisée.

En outre, en raison de l'absence d'obligation de motivation, le texte ne fait aucune distinction entre une vérification superficielle et une enquête complète. En cas de vérification sommaire, des informations complémentaires seront demandées. En revanche, une enquête

huiszoekingen of vorderingen van bankgegevens. De bepaling stelt enkel dat er een controle zal worden uitgevoerd, waardoor een modelrisico onmiddellijk kan omslaan in een volledig controleproces, zonder enige drempel of proportionaliteitsafweging. In het klassieke systeem beslist een controleur zelf of een signaal voldoende ernstig is om een controle te openen. In het voorgestelde systeem beslist het algoritme, terwijl de mens enkel nog de uitvoering verzorgt.

Vervolgens wijst de heer Van Quickenborne erop dat men evolueert van risicobeoordeling naar wat men noemt *algorithmic enforcement*. Dit betekent dat de overheid algoritmen niet langer enkel inzet om prioriteiten te bepalen, maar ook om daadwerkelijke handhaving te initiëren. Het startpunt is hierbij niet langer menselijk inzicht, maar statistische waarschijnlijkheid. Er is bovendien geen wettelijk vastgelegde drempel, terwijl de beslissing tot actie wel materiële gevolgen heeft voor individuele burgers. Precies dit acht het Hof van Justitie onverenigbaar met het Unierecht.

In het fiscale recht is bovendien de selectie van dossiers voor controle een discretionaire bevoegdheid. Die moet worden uitgeoefend binnen het kader van het gelijkheidsbeginsel en het motiveringsbeginsel. Volgens de spreker wordt deze bevoegdheid door het amendement gedelegeerd aan een algoritme. Dat algoritme bepaalt wie verdacht is en wie een controle krijgt. Formeel blijven ambtenaren wel beslissen, maar feitelijk worden zij gereduceerd tot uitvoerders van wat het systeem bepaalt. Het lid besluit dat dit de verhouding tussen burger en overheid fundamenteel aantast.

De heer Van Quickenborne gaat vervolgens in op de risicofactoren die in het vijfde lid worden opgesomd en bespreekt de praktische implicaties daarvan. Hij merkt op dat elk controlemodel onvermijdelijk valse positieven genereert: burgers die ten onrechte als risico worden aangemerkt en daardoor een onrechtmatige controle krijgen. Zonder voorafgaande menselijke filtering worden dergelijke fouten niet rechtgezet.

Daarnaast wijst het commissielid op de gevaren van het gebruik van socio-economische proxy's als risicofactor, zoals beroepscategorie of migratieachtergrond. Wanneer dergelijke elementen deel uitmaken van de selectiecriteria in het kader van *money control*, bestaat het risico dat bepaalde groepen structureel en onzichtbaar worden gediscrimineerd. Zelfs zonder dat dit leidt tot een sanctie, kan een controle op zich al aanzienlijke reputatieschade veroorzaken.

complette pourra donner lieu à des perquisitions ou à des demandes de données bancaires. La disposition indique uniquement qu'un contrôle aura lieu, ce qui signifie qu'un modèle de risque pourra se muer immédiatement en un processus de contrôle complet, sans aucun seuil ni appréciation de la proportionnalité. Dans le système classique, un contrôleur détermine si un signal est suffisamment grave pour justifier un contrôle. Dans le système proposé, l'algorithme décidera, tandis que l'être humain ne se chargera plus que de l'exécution.

M. Van Quickenborne souligne ensuite que l'on passera de l'évaluation des risques à une application algorithmique (*algorithmic enforcement*). Cela signifie que les pouvoirs publics n'utiliseront plus les algorithmes uniquement pour définir des priorités, mais aussi pour entamer un contrôle effectif du respect de la loi. Ce ne sera plus l'appréciation humaine mais bien la probabilité statistique qui sera à l'origine de ce processus. De plus, aucun seuil ne sera fixé par la loi, alors que la décision d'agir aura des conséquences matérielles pour les citoyens individuels. C'est précisément ce que la Cour de justice juge incompatible avec le droit de l'Union.

En droit fiscal, la sélection des dossiers à contrôler relève en outre d'une compétence discrétionnaire qui doit être exercée conformément aux principes d'égalité et de motivation. L'intervenant estime que l'amendement à l'examen prévoit de déléguer cette compétence à un algorithme qui déterminera qui sera suspect et contrôlé. Formellement, les agents du fisc continueront à décider, mais, en pratique, ils seront réduits au rôle d'exécutants de ce que le système aura établi. Le membre conclut en indiquant que cela portera fondamentalement atteinte à la relation entre les citoyens et les pouvoirs publics.

M. Van Quickenborne aborde ensuite la question des facteurs de risque énumérés dans l'alinéa 5, et examine leurs implications pratiques. Il fait observer que tout modèle de contrôle génère inévitablement des faux positifs concernant des citoyens erronément considérés comme présentant un risque et qui font donc l'objet d'un contrôle illégitime. Sans filtrage humain préalable, les erreurs de cette nature ne seront pas corrigées.

Le membre pointe par ailleurs les dangers de l'utilisation d'indicateurs socioéconomiques de substitution, tels que la catégorie professionnelle ou une origine immigrée, en tant que facteur de risques. Si ces éléments font partie des critères de sélection dans le cadre du *money control*, certains groupes de personnes risquent de faire l'objet d'une discrimination structurelle et invisible. Même lorsqu'il n'entraîne aucune sanction, un contrôle peut en soi nuire considérablement à la réputation.

De spreker vergelijkt vervolgens het voorgestelde systeem van *money control* met het klassieke controlesysteem. De vraag rijst immers: wie beslist over het openen van een controle? In het traditionele model neemt een controleur, eventueel in overleg met zijn leidinggevende, die beslissing. In het systeem van *money control* wordt de beslissing echter genomen door een algoritme binnen een data-afdeling.

Verder is er in een klassieke controle steeds sprake van een motivering en ontvangt de betrokken belastingplichtige een kennisgeving, bijvoorbeeld via een brief of een aankondiging. Binnen *money control* ontbreekt zowel de motivering als de kennisgeving. De burger krijgt bovendien geen mogelijkheid tot betwisting, omdat hij niet wordt geïnformeerd over de selectie, de gebruikte criteria of de aanleiding. Enkel in het klassieke systeem bestaat achteraf nog een mogelijkheid tot bezwaar of klacht.

Wanneer men het vijfde lid toetst aan artikel 22 van de GDPR en de relevante EU-rechtspraak, zo stelt het lid, dan moet worden vastgesteld dat het systeem rechtstreeks strijdig is met deze bepalingen. Ook artikel 170 van de GDPR komt in het gedrang. Er is immers geen voorafgaande menselijke verificatie van de controleopdracht en geen onafhankelijke toetsing achteraf, waardoor het juridische risico aanzienlijk is.

Tot slot bevat het vijfde lid geen verplicht register van depseudonimiseringshandelingen of controleopdrachten, geen interne of externe auditverplichting en kent het geen rol toe aan de DPO of de GBA in het toezicht op de selectieprocessen. Daardoor verloopt de handhaving volledig ondergeschikt aan het algoritme, zonder voldoende waarborgen voor de rechtsbescherming.

De heer Van Quickenborne licht toe hoe het vijfde lid in overeenstemming kan worden gebracht met de grondrechten en het Europese Unierecht. Volgens het commissielid vergt het dat er minstens een aantal bijkomende waarborgen worden gesteld.

Ten eerste moet een fiscale ambtenaar de modeloutput beoordelen en schriftelijk motiveren waarom de gepersonaliseerde score aanleiding geeft tot een controle. Ten tweede moet deze beslissing worden gevalideerd door een leidinggevende of door een *data governance board*. Ten derde moet elke controle die voortvloeit uit een algoritmisch proces worden opgenomen in een register dat jaarlijks wordt overgemaakt aan de GBA. Ten vierde moeten burgers na afsluiting van het onderzoek het recht krijgen te vernemen of hun dossier via

L'intervenant compare ensuite le système proposé du "*money control*" au système de contrôle classique. La question se pose en effet de savoir qui décide d'entreprendre un contrôle. Dans le modèle traditionnel, cette décision est prise par un contrôleur, éventuellement en concertation avec son supérieur hiérarchique. En revanche, dans le système du "*money control*", cette décision sera prise par un algorithme dans un service de traitement de données.

En outre, dans le cadre d'un contrôle classique, il y a toujours une motivation et le contribuable visé est informé, par exemple par courrier ou par la voie d'une notification. Dans le "*money control*", tant la motivation que la notification feront défaut. Qui plus est, le citoyen ne se verra accorder aucune possibilité de contestation, car il ne sera pas informé de la sélection, des critères utilisés ou du motif. Seul le système classique permet d'introduire une réclamation ou une plainte *a posteriori*.

Selon l'intervenant, quand on examine l'alinéa 5 à la lumière de l'article 22 du RGPD et de la jurisprudence européenne pertinente, on n'a pas d'autre choix que de constater que ce système est diamétralement contraire à ces dispositions. L'article 170 du RGPD sera également enfreint. La mission de contrôle ne sera en effet soumise ni à une vérification humaine préalable ni à une évaluation indépendante *a posteriori*, si bien que le risque juridique est considérable.

Enfin, l'alinéa 5 ne prévoit ni l'obligation de tenir un registre des actes de depseudonymisation ou des missions de contrôle, ni l'obligation de procéder à un audit interne ou externe, et il ne confère aucun rôle de contrôle des processus de sélection au DPO ou à l'APD. Il s'ensuit que l'application de la législation sera entièrement soumise à l'algorithme, sans garanties suffisantes en matière de protection juridique.

M. Van Quickenborne explique comment l'alinéa 5 peut être mis en conformité avec les droits fondamentaux et le droit de l'Union européenne. Selon le membre, il est nécessaire de prévoir diverses garanties supplémentaires à cet effet.

Premièrement, un agent du fisc doit examiner le résultat du modèle et justifier par écrit pourquoi le score personnalisé donne lieu à un contrôle. Deuxièmement, cette décision doit être validée par un supérieur hiérarchique ou par un *data governance board*. Troisièmement, tout contrôle résultant d'un processus algorithmique doit être inscrit dans un registre transmis chaque année à l'APD. Quatrièmement, les citoyens doivent, après la clôture de l'enquête, avoir le droit de savoir si leur dossier a été ouvert par sélection algorithmique, et sur la base

algoritmische selectie werd geopend en op basis van welke risicofactoren dit gebeurde. Ten slotte moet de formulering uit het vijfde lid “zal worden gevraagd” worden vervangen door “kan worden gevraagd na menselijke beoordeling en een gemotiveerde beslissing”.

De spreker beschouwt dit alles als noodzakelijke verbeteringen en kondigt aan dat de Open Vld een amendement in deze zin zal indienen, tenzij de minister bevestigt dat de bepaling reeds op de besproken wijze moet worden geïnterpreteerd of bereid is de tekst overeenkomstig aan te passen.

De heer Van Quickenborne vat de kernproblematiek omtrent het vijfde lid samen: de automatische koppeling tussen een modelscore en de opening van een controle, zonder menselijke toetsing, vormt een schending van artikel 22 GDPR. Daarnaast ontbreekt een motiveringsplicht, wat in strijd is met artikelen 10 en 11 van de Grondwet. Het ontbreken van kennisgeving en beroepsmogelijkheden ontnemt de burger een effectieve rechtsbescherming, wat een schending vormt van artikel 47 van het Handvest van de grondrechten van de EU. Het ontbreken van onafhankelijk toezicht ontnemt elke rem op de data-afdeling, waardoor het systeem onverenigbaar wordt met het Unierecht. De gebruikte terminologie, zoals “zal worden gevraagd”, laat bovendien geen discretionaire marge en is te vaag geformuleerd om rechtszekerheid te bieden.

Volgens het commissielid lijkt het vijfde lid op het eerste gezicht een louter procedurele bepaling, maar vormt het in werkelijkheid de juridische schakel die van *money control* een systeem van geautomatiseerde handhaving maakt. Het vijfde lid schendt verschillende fundamentele beginselen, waaronder proportionaliteit, transparantie en het recht op een eerlijk proces. In essentie, zo stelt de spreker, is dit het moment waarop de fiscus stopt met oordelen en begint te gehoorzamen aan een model. Daarmee verlaat *money control* het terrein van de klassieke fiscaliteit en betreedt het de sfeer van wat het lid omschrijft als “de geautomatiseerde macht”.

Wat betreft het zesde lid, van het nieuwe artikel 95/3 dat werd ingevoegd door amendement nr. 16 (DOC 56 0963/005) in eerste lezing (DOC 56 0963/020), licht de heer Van Quickenborne toe dat de concrete gegevens afkomstig van het CAP, die overeenkomstig het eerste lid worden verwerkt, niet mogen worden meege-deeld aan de ambtenaar die de controle uitvoert, tenzij is voldaan aan de voorwaarden van artikel 322 WIB.

de quels facteurs de risque. Enfin, en ce qui concerne la formulation de l’alinéa 5, il convient de remplacer “il sera alors demandé au service de contrôle compétent d’effectuer une vérification du dossier sélectionné” par “il pourra alors être demandé au service de contrôle compétent d’effectuer une vérification du dossier sélectionné après une évaluation humaine et une décision motivée”.

L’intervenant considère l’ensemble de ces mesures comme des améliorations nécessaires et annonce que l’Open Vld présentera un amendement en ce sens, sauf si le ministre confirme que la disposition doit être interprétée de la manière évoquée ou s’il est disposé à modifier le texte en conséquence.

M. Van Quickenborne résume le principal problème posé par l’alinéa 5: le lien automatique entre un score de modèle et l’ouverture d’un contrôle, sans évaluation humaine, constitue une violation de l’article 22 du RGPD. En outre, l’absence d’obligation de motivation est contraire aux articles 10 et 11 de la Constitution. L’absence de notification et de voies de recours prive le citoyen d’une protection juridictionnelle effective, ce qui constitue une violation de l’article 47 de la Charte des droits fondamentaux de l’Union européenne. L’absence de contrôle indépendant laisse toute liberté au service chargé des données, rendant ainsi le système incompatible avec le droit de l’Union. La terminologie utilisée, telle que “il sera alors demandé au service de contrôle compétent d’effectuer une vérification”, ne laisse par ailleurs aucune marge discrétionnaire et est formulée de manière trop vague pour garantir la sécurité juridique.

Selon le membre, l’alinéa 5 semble être, à première vue, une disposition purement procédurale, mais constitue en réalité le chaînon juridique qui transforme le *money control* en un système de contrôle automatisé. L’alinéa 5 viole plusieurs principes fondamentaux, dont la proportionnalité, la transparence et le droit à un procès équitable. En substance, comme le souligne l’intervenant, le fisc cessera alors de procéder à une évaluation et commencera à obéir à un modèle. Ce faisant, le *money control* quittera le terrain de la fiscalité classique et entrera dans la sphère que le membre qualifie de “pouvoir automatisé”.

En ce qui concerne l’alinéa 6 du nouvel article 95/3, inséré par l’amendement n° 16 (DOC 56 0963/005) en première lecture (DOC 56 0963/020), M. Van Quickenborne explique que les données concrètes provenant du PCC qui seront traitées conformément à l’alinéa 1^{er}, ne pourront être communiquées au fonctionnaire chargé du contrôle, sauf si les conditions prévues par l’article 322 CIR sont remplies.

Op het eerste gezicht bevat deze zin twee elementen. Enerzijds is er de hoofdregel dat concrete CAP-gegevens, zoals bankinformatie, contracten en saldi, niet aan de controleambtenaar mogen worden meegedeeld. Anderzijds is er een uitzondering, namelijk wanneer voldaan is aan de klassieke bevoegdheidsvoorwaarden van artikel 322 WIB. Op papier lijkt dit een sterke bescherming te bieden: de gewone controleur mag de bankinformatie pas inkijken na een getrappt proces, bestaande uit een vermoeden van fraude, het vaststellen van onwil tot medewerking en pas vervolgens de toegang tot het CAP.

In toepassing van artikel 46.2. van het Kamerreglement, betreffende de herhaling van argumenten door eenzelfde lid, heeft de voorzitter het woord ontnomen van de heren Vincent Van Quickenborne (Open Vld) en Lode Vereeck (VB).

Op vraag van mevrouw Charlotte Verkeyn (N-VA) heeft de voorzitter de intentie geuit om artikel 53 van het Kamerreglement, betreffende de sluiting van de bespreking, aan te wenden. Uiteindelijk werd het artikel niet toegepast.

Na een proceduredebat met tussenkomsten van de heren Vincent Van Quickenborne (Open Vld), Lode Vereeck (VB), Khalil Aouasti (PS), Wim Van der Donckt (N-VA) en de dames Alexia Bertrand (Open Vld) en Sofie Merckx (PVDA-PTB) heeft de voorzitter de vergadering beëindigd.

B. Antwoorden van de minister

De heer Jan Jambon, vice-eersteminister en minister van Financiën en Pensioenen, belast met de Nationale Loterij en de Federale Culturele Instellingen, merkt op dat tweede lezing begonnen is op 21 oktober 2025. Nadien werden er nog vier vergaderingen aan de tweede lezing gewijd. Vandaag is het dus de zesde vergadering.

De minister benadrukt dat hij alles in het werk stelt om zeer concreet op de vele vragen te antwoorden.

1. De flexi-jobs

Zoals de minister reeds tijdens de eerste lezing heeft aangegeven is er op flexi-jobs een patronale bijdrage van 28 % verschuldigd. De minister blijft dan ook achter het systeem van de flexi-jobs staan. De flexi-jobs vullen een reële nood aan op de arbeidsmarkt en laten de mensen toe iets extra te kunnen verdienen aan gunstige voorwaarden.

Au premier abord, cette phrase contient deux éléments. D'une part, il y a la règle principale selon laquelle les données concrètes du PCC, telles que les informations bancaires, les contrats et les soldes, ne pourront être communiquées au fonctionnaire chargé du contrôle. D'autre part, une exception est prévue, à savoir lorsque les conditions classiques de compétence prévues par l'article 322 CIR sont respectées. Sur le papier, cette disposition semble offrir une protection solide: le contrôleur ordinaire ne pourra consulter les informations bancaires qu'après un processus graduel, à savoir un soupçon de fraude suivi de la constatation que l'intéressé refuse de coopérer, puis seulement l'accès au PCC.

En application de l'article 46.2., du Règlement de la Chambre, qui vise la situation où un même membre répète les mêmes arguments, le président retire la parole à MM. Vincent Van Quickenborne (Open Vld) et Lode Vereeck (VB).

À la demande de Mme Charlotte Verkeyn (N-VA), le président exprime l'intention de recourir à l'article 53 du Règlement de la Chambre, relatif à la clôture de la discussion. Finalement, cet article n'est pas appliqué.

Après un débat de procédure marqué par des interventions de MM. Vincent Van Quickenborne (Open Vld), Lode Vereeck (VB), Khalil Aouasti (PS), Wim Van der Donckt (N-VA) et de Mmes Alexia Bertrand (Open Vld) et Sofie Merckx (PTB), le président clôture la réunion.

B. Réponses du ministre

M. Jan Jambon, vice-premier ministre et ministre des Finances et des Pensions, chargé de la Loterie Nationale et des Institutions culturelles fédérales, fait observer que la deuxième lecture a débuté le 21 octobre 2025. Quatre réunions supplémentaires y ont ensuite été consacrées. Il s'agit donc aujourd'hui de la sixième réunion.

Le ministre souligne qu'il mettra tout en œuvre pour répondre de manière très concrète aux nombreuses questions.

1. Les flexi-jobs

Comme le ministre l'a déjà indiqué lors de la première lecture, les flexi-jobs sont soumis à une cotisation patronale de 28 %. Le ministre continue donc de soutenir le système des flexi-jobs. Ceux-ci répondent à un besoin réel sur le marché du travail et permettent aux travailleurs concernés de percevoir un complément de revenus à des conditions avantageuses.

De parafiscale ontvangsten inzake de flexi-jobs kunnen worden opgevraagd bij de bevoegde minister. Op een flexi-job is namelijk enkel een patronale socialezekerheidsbijdrage verschuldigd, geen personenbelasting.

2. De opmerkingen in het advies van de Raad van State over “staatssteun”

De minister antwoordt dat dit wetsontwerp de fiscaal vrijgestelde drempel van 12.000 euro voor flexi-jobs wenst op te trekken naar 18.000 euro voor dit inkomstenjaar. De uitbreiding naar alle sectoren ligt niet op tafel in deze commissie, dat zal in de commissie voor Sociale Zaken besproken worden.

De minister is van mening dat het optrekken van het plafond naar 18.000 euro geen staatssteun is. Sommige commissieleden hebben opgemerkt dat de Raad van State geen advies heeft gegeven over deze mogelijke staatssteunproblematiek. Dit is echter niet juist, de Raad van State heeft daar wel degelijk een advies over gegeven (DOC 56 0963/001, p. 416). De Raad van State heeft de fiscale regel in het wetsontwerp namelijk getoetst aan de zogenaamde “de-minimissteun”.

De minister refereert ook naar het arrest van 28 september 2017 van het Grondwettelijk Hof waarbij werd aangehaald dat flexi-jobs ongrondwettelijk zijn omdat ze discrimineren ten opzicht van normale werknemers doordat er minder lasten zijn. Op een flexi-loon is er namelijk geen personenbelasting verschuldigd. Het Grondwettelijk Hof oordeelde uiteindelijk dat er geen discriminatie was, toen was er bovendien nog geen fiscaal plafond. Door de vorige regering werd een niet-geïndexeerd plafondbedrag ingevoerd, dat plafond wordt nu verhoogd en zal ook geïndexeerd worden.

Verder komt het fiscale voordeel enkel ten goede aan natuurlijke personen die geen onderneming zijn. Het bestaan van een fiscaal voordeel voor de betrokken werknemers ontslaat de werkgever niet van de verplichting om lonen te betalen overeenkomstig de sectorale bepalingen, noch van de naleving van de toepasselijke arbeidsrechtelijke en sociale zekerheidsregels.

Om te kunnen spreken van staatssteun moet er een beïnvloeding zijn van het handelsverkeer en de mededinging. Het handelsverkeer tussen de lidstaten moet ongunstig beïnvloed worden. Het is moeilijk te argumenteren dat flexi-jobs ervoor zouden zorgen dat Belgische ondernemingen plots het intracommunautaire handelsverkeer gaan beïnvloeden. De Europese Commissie heeft in diverse zaken geconcludeerd dat bepaalde activiteiten, door de specifieke omstandigheden ervan, een zuiver lokaal

Les informations concernant les recettes parafiscales relatives aux flexi-jobs peuvent être demandées auprès du ministre compétent. En effet, les flexi-jobs sont uniquement soumis à une cotisation patronale de sécurité sociale, et non à l'impôt des personnes physiques.

2. Les observations relatives à l’“aide d’État” dans l’avis du Conseil d’État

Le ministre répond que le projet de loi à l'examen vise à relever le seuil exonéré d'impôt pour les flexi-jobs de 12.000 euros à 18.000 euros pour l'année de revenus en cours. L'extension à tous les secteurs n'est pas à l'ordre du jour de cette commission. Elle sera examinée en commission des Affaires sociales.

Le ministre estime que le relèvement du plafond à 18.000 euros ne constitue pas une aide d'État. Certains membres de la commission ont fait observer que le Conseil d'État n'avait pas rendu d'avis sur cette problématique potentielle. Ce n'est pas exact, car le Conseil d'État a bel et bien rendu un avis à ce sujet (DOC 56 0963/001, p. 416). Le Conseil d'État a en effet examiné la règle fiscale prévue dans le projet de loi au regard de la notion d’“aides de minimis”.

Le ministre fait également référence à l'arrêt rendu le 28 septembre 2017 par la Cour constitutionnelle, qui s'est prononcée sur le caractère prétendument inconstitutionnel des flexi-jobs, qui constitueraient une discrimination à l'égard des travailleurs ordinaires en raison des charges moindres qui leur sont applicables. En effet, les flexi-salaires ne sont pas soumis à l'impôt des personnes physiques. La Cour constitutionnelle a finalement considéré qu'il n'y avait pas de discrimination, alors qu'à l'époque, il n'y avait même pas encore de plafond fiscal. Le gouvernement précédent a introduit un plafond non indexé, qui sera à présent relevé et indexé.

En outre, l'avantage fiscal ne profite qu'aux personnes physiques qui ne sont pas des entreprises. L'existence d'un avantage fiscal pour les travailleurs concernés ne dispense pas l'employeur de l'obligation de payer les rémunérations conformément aux dispositions sectorielles, ni de respecter les règles applicables en matière de droit du travail et de sécurité sociale.

Pour pouvoir parler d'aide d'État, il faut qu'il y ait une influence sur les échanges commerciaux et la concurrence. Les échanges commerciaux entre États membres doivent être affectés de manière défavorable. On peut difficilement affirmer qu'à cause des flexi-jobs, les entreprises belges auraient soudainement une influence sur les échanges commerciaux intracommunautaires. La Commission européenne a conclu dans plusieurs affaires que certaines activités, en raison des circonstances

karakter hadden en het handelsverkeer tussen lidstaten niet ongunstig beïnvloeden. Bij flexi-jobs gaat het om een marginaal effect op de intracommunautaire markt.

3. *De hybride wagens*

De versoepeling voor hybride wagens zal enkel gelden voor eenmanszaken-natuurlijke personen. Dat heeft de minister al uitgebreid toegelicht.

Er werd daarover een moeizaam compromis met de Europese commissie bereikt en er werd een compromis gemaakt binnen de regering. Dat compromis ligt hier voor ter stemming. Er is nadien geen contact meer geweest met de Europese Commissie.

De autofiscaliteit werd grondig aangepast in de vorige legislatuur. Het is voor de minister belangrijk dat daar nu de nodige stabiliteit in komt, zowel voor de ondernemingen als voor de werknemers.

4. *De vrijstelling inzake de PC-Privé*

De minister geeft aan dat het hier concreet gaat om de vrijstelling van belasting van de tussenkomst van een werkgever in de aankoop van een PC privé. Deze vrijstelling wordt nu opgeheven met ingang van 1 oktober 2025, dat is het begin van het vierde kwartaal omdat dit ook zo doorwerkt op het vlak van de sociale zekerheid en daar dient er per kwartaal gewerkt te worden.

Voor de volledigheid geeft de minister nog graag de fiscale uitgaven mee van tijdens het aanslagjaar 2024. Voor Vlaanderen ging het om een fiscale uitgave van 26.000 euro, voor Wallonië 15.000 euro en voor Brussel 12.000 euro. In totaal ging het dus om een fiscale uitgave van 53.000 euro die nu wordt afgeschaft. Samengeteld gaat het om circa 1.500 belastingplichtigen.

5. *Het aanslagjaar special*

Zuiver inhoudelijk en ter aanvulling van wat er reeds is gezegd geweest bij de eerste lezing, verduidelijkt de minister nog even waarom de meeste wijzigingen in werking treden met ingang van aanslagjaar 2026 en andere wijzigingen een welbepaalde datum meekrijgen als startpunt van de inwerkingtreding en dit in het licht van het zogenaamde aanslagjaar 2025 speciaal

Om te beginnen bij het begin: voor al wie in België woont en hier het hele jaar blijft wonen, is het aanslagjaar

specifiek in de context van de hybride wagens, hadden specifieke dans lesquelles elles s'inscrivaient, avaient un caractère purement local et n'affectaient pas défavorablement les échanges commerciaux entre États membres. Dans le cas des flexi-jobs, l'effet sur le marché intracommunautaire est marginal.

3. *Les véhicules hybrides*

Comme le ministre l'a déjà expliqué de manière détaillée, l'assouplissement pour les véhicules hybrides ne s'appliquera qu'aux entreprises individuelles (personnes physiques).

Un compromis laborieux a été dégagé avec la Commission européenne à ce sujet. Un compromis a également été conclu au sein du gouvernement. Il est actuellement soumis au vote. Il n'y a plus eu de contact avec la Commission européenne depuis lors.

La fiscalité automobile a été profondément remaniée lors de la législature précédente. Pour le ministre, il importe d'instaurer désormais la stabilité nécessaire en la matière, tant pour les entreprises que pour les travailleurs.

4. *L'exonération pour le PC privé*

Le ministre précise qu'il s'agit concrètement de l'exonération fiscale de l'intervention de l'employeur dans le prix d'achat d'un PC privé. Cette exonération sera abrogée à compter du 1^{er} octobre 2025, soit au début du quatrième trimestre, car elle a également des répercussions sur le plan de la sécurité sociale, où les calculs doivent être effectués par trimestre.

Pour être complet, le ministre souhaite également communiquer les dépenses fiscales y afférentes pour l'exercice d'imposition 2024. Pour la Flandre, la dépense fiscale s'élevait à 26.000 euros, pour la Wallonie à 15.000 euros et pour Bruxelles à 12.000 euros. Au total, la dépense fiscale était donc de 53.000 euros. Elle sera désormais supprimée. Au total, cette mesure concerne environ 1.500 contribuables.

5. *L'exercice d'imposition spécial*

Sur le plan du contenu et pour compléter ce qui a déjà été dit lors de la première lecture, le ministre explique encore brièvement pourquoi la plupart des modifications entreront en vigueur à partir de l'exercice d'imposition 2026 et pourquoi d'autres modifications entreront en vigueur à une date précise. Cette différence est liée à l'exercice d'imposition spécial 2025.

Le ministre rappelle tout d'abord que, pour toute personne résidant en Belgique et y demeurant toute

gelijk aan het inkomstenjaar +1. Aanslagjaar 2026 heeft dus bijvoorbeeld betrekking op inkomstenjaar 2025.

Een maatregel die in werking treedt met ingang van aanslagjaar 2026, treedt dus in werking op 1 januari 2025. Het gaat hier niet om terugwerkende kracht zoals de Raad van State al meermaals heeft gezegd, want het belastbaar tijdperk (het inkomstenjaar dus) is nog niet voorbij. Het bovenstaande geldt dus voor wie in België woont en hier op 31 december 2025 nog altijd woont.

Anders wordt het voor iemand die in België woont maar voor wie de zogenaamde gronden van belastbaarheid weggevallen zijn voor 31 december 2025. Concreet gaat het dan om iemand die verhuist naar een ander land voor 31 december 2025.

In dat geval is men op 31 december 2025 niet meer belastbaar in België en bijgevolg moet men nog wel een aangifte voor de inkomstenbelasting indienen, tot net voor de datum van verhuizing.

Voorbeeld: iemand verhuist op 1 september definitief naar Luxemburg. Hij zal voor de periode van 1 januari 2025 tot 31 augustus 2025 dan nog een aangifte inkomstenbelasting moeten indienen in België.

Welnu, een aangifte die niet loopt tot 31 december van het jaar, noemt men een aangifte speciaal. Concreet, wie verhuist op 1 september 2025, moet nog een aangifte 2025 speciaal indienen.

Een maatregel die in werking treedt vanaf het aanslagjaar 2026 is niet van toepassing op een belastingplichtige die in de loop van het jaar is verhuisd, aangezien deze geen aangifte meer moet indienen voor het aanslagjaar 2026, maar wel een aangifte speciaal voor het aanslagjaar 2025.

In veel gevallen maakt dit weinig of geen verschil. Maar het is soms belangrijk erop toe te zien dat er geen ongelijke behandeling ontstaat tussen belastingplichtigen die in België blijven en effectief onderworpen zijn aan een maatregel die ingaat vanaf het aanslagjaar 2026, en zij die in 2025 zijn verhuisd en geen aangifte meer moeten indienen voor het aanslagjaar 2026, maar wel een aangifte speciaal voor 2025.

l'année, l'exercice d'imposition correspond à l'année de revenus +1. Par exemple, l'exercice d'imposition 2026 concerne donc l'année de revenus 2025.

Une mesure qui entre en vigueur à compter de l'exercice d'imposition 2026 prendra donc effet au 1^{er} janvier 2025. Il ne s'agit pas d'une mesure rétroactive, comme l'a déjà indiqué à plusieurs reprises le Conseil d'État, car la période imposable (c'est-à-dire l'année de revenus) n'est pas encore terminée. Ce qui précède s'applique donc à toute personne qui réside en Belgique et qui y réside toujours au 31 décembre 2025.

La situation est différente pour les personnes qui résident en Belgique mais pour lesquelles les conditions d'assujettissement ont disparu avant le 31 décembre 2025. Concrètement, il s'agit des personnes qui déménagent dans un autre pays avant le 31 décembre 2025.

Ces personnes ne seront alors plus imposables en Belgique au 31 décembre 2025 et elles devront donc encore introduire une déclaration d'impôt pour la période s'écoulant jusque juste avant la date du déménagement.

Par exemple, une personne déménage définitivement au Luxembourg le 1^{er} septembre. Elle devra encore introduire une déclaration d'impôt en Belgique pour la période comprise entre le 1^{er} janvier 2025 et le 31 août 2025.

Une déclaration qui ne court pas jusqu'au 31 décembre de l'année est appelée déclaration spéciale. Concrètement, la personne qui déménage le 1^{er} septembre 2025 doit encore introduire une déclaration spéciale 2025.

Une mesure qui entre en vigueur à partir de l'exercice d'imposition 2026 ne s'applique pas à un contribuable qui a déménagé au cours de l'année 2025, car celui-ci ne doit pas introduire de déclaration pour l'exercice d'imposition 2026, mais bien une déclaration spéciale pour l'exercice d'imposition 2025.

Dans de nombreux cas, cela ne fait guère de différence, voire aucune. Mais il peut être important de veiller à éviter tout inégalité de traitement entre les contribuables qui restent en Belgique et qui sont effectivement soumis à une mesure qui entre en vigueur à partir de l'exercice d'imposition 2026, et ceux qui ont déménagé en 2025 et qui ne doivent pas introduire de déclaration pour l'exercice d'imposition 2026, mais bien une déclaration spéciale pour 2025.

6. Het CAP

Er waren beschouwingen over de GDPR, het EVRM, het Handvest van de grondrechten van de Europese Unie en er was ook een rechtsvergelijkende analyse.

Daarnaast ging het in deze commissie heel uitgebreid over het Europese voorstel tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen. De minister zal zich over dat Europese voorstel niet uitspreken aangezien dit tot de bevoegdheid behoort van het Europese Parlement en niet tot de bevoegdheid van het federale parlement.

De minister zal zich in zijn antwoord beperken tot de artikelen in dit wetsontwerp en zal proberen uitgebreid te antwoorden op de vele vragen en opmerkingen.

Vooreerst schetst hij een korte historiek van het dossier.

Het CAP ontstond in 2011 om fiscale fraude te bestrijden met de wet houdende diverse bepalingen van 14 april 2011.

De minister verwijst naar het verslag van bespreking van dat wetsontwerp in 2011. Een Kamerlid zie toen dat dit “(wetsontwerp) *de belastingadministratie de mogelijkheid zal geven om haar werk te doen en de belastingen correct heffen*” en “*belastingontduiking doeltreffender te bestrijden*” (DOC 53 1208/012, p. 37).

Welnu, dat is nog steeds het geval, want fiscale fraude raakt immers ook de eerlijke burger en ondernemer.

Sinds 2015 moeten belastingplichtigen met een rekening in het buitenland die melden aan het CAP

In 2018 kwam er een uitbreiding van het aantal instellingen die het CAP kunnen consulteren

In 2020 werd het CAP uitgebreid met de halfjaarlijkse mededeling van alle banksaldi en van het globaal bedrag van bepaalde soorten financiële contracten, met name spaarverzekeringen en investeringscontracten.

De minister benadrukt dat het gaat om de banksaldi, niet om de verrichtingen, zoals hier, en ook elders, verschillende keren verkeerdelijk werd gesteld.

De minister merkt op dat sommige commissieleden het probeerden voor te stellen alsof het nieuw is dat “alle

6. Le PCC

Il a été tenu compte du RGPD, de la ConvEDH, de la Charte des droits fondamentaux de l'Union européenne et il a été procédé à une analyse de droit comparé.

Par ailleurs, la commission a longuement débattu de la proposition du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants. Le ministre ne se prononcera pas sur cette proposition, car elle relève de la compétence du Parlement européen, et pas de celle du Parlement fédéral.

Dans sa réponse, le ministre se limitera aux articles du projet de loi à l'examen et s'efforcera de répondre de manière détaillée aux nombreuses questions et observations.

Il retracera d'abord brièvement la genèse du dossier.

Le PCC a été créé en 2011 par la loi du 14 avril 2011 portant des dispositions diverses, afin de lutter contre la fraude fiscale.

Le ministre renvoie au rapport relatif aux discussions organisées en 2011 à propos de ce projet de loi. Un député avait alors estimé que ce “[projet de loi permettrait] à l'administration fiscale de faire son travail et de lever les impôts correctement” et “de lutter efficacement contre la fraude fiscale” (DOC 53 1208/012, p. 37).

Or, cette observation est toujours d'actualité, car la fraude fiscale touche effectivement aussi les citoyens et les entrepreneurs honnêtes.

Depuis 2015, les contribuables titulaires d'un compte à l'étranger doivent déclarer ce compte au PCC.

En 2018, l'accès au PCC a été élargi à d'autres institutions.

En 2020, la liste des données à communiquer au PCC a été étoffée, pour y inclure la communication semestrielle de tous les soldes des comptes bancaires et du montant global de certains types de contrats financiers, notamment les assurances épargne et les contrats d'investissement.

Le ministre souligne qu'il s'agit des soldes des comptes bancaires, et pas des opérations bancaires comme d'aucuns l'ont affirmé à plusieurs reprises et à tort au sein de la commission et ailleurs.

Le ministre fait observer que certains membres de la commission ont tenté de présenter comme une nouveauté

saldi van bankrekeningen in het CAP zitten". Dat is dus niet nieuw. Er is volgens de minister een opmerkelijke selectiviteit in het geheugen van sommige commissieleden. Deze beslissing werd genomen door de vorige regering en dateert van 2020.

Vervolgens legt de minister uit wat er nu verandert met dit wetsontwerp. Conform het regeerakkoord wordt er een wettelijk kader gecreëerd voor datamining op de gepseudonimiseerde gegevens uit het CAP met het oog op dossierselectie.

Waar vroeger een ervaren ambtenaar dossiers, al bladerend door de fichebak, selecteert op basis van zijn ervaring om ze grondig na te kijken, zal dit nu ook gebeuren door anonieme datamining.

Tevens moeten effecten- en cryptorekeningen individueel bij het CAP worden aangemeld.

— *Met betrekking tot de opmerkingen inzake privacy:*

De minister verwijst naar de garanties voorzien voor de belastingplichtigen inzake gegevensverwerking, uit de wet van 3 augustus 2012. De minister benadrukt dat er aan deze bepalingen helemaal niets wordt gewijzigd.

De minister beklemtoont tevens dat de gegevens enkel worden gebruikt om efficiëntere risicoanalyses mogelijk te maken en dossiers efficiënt te selecteren. Die risicoanalyses worden voor advies voorgelegd aan een "Data Protection Officer" in de zogenaamde DAM-fiche.

De DAM-fiche wordt gebruikt om het specifieke dataminingproject te documenteren – het beschrijft het project, het doel ervan, de databases die zullen worden gebruikt, en de dataminers die er toegang toe zullen hebben. Dit maakt het mogelijk om de rechtsgrond te verifiëren en de proportionaliteit van de gebruikte gegevens te beoordelen. Het stelt de FOD Financiën dus in staat zijn GDPR-verplichtingen na te leven.

In deze DAM-fiche zitten de parameters die gericht zijn op inbreuken op fiscale wetgeving. Die parameters maken, zoals de minister vorige keer reeds heeft gezegd, deel uit van de interne strategie van de FOD Financiën.

Verder gaat de minister in op de opmerking dat dit een schending van de openbaarheid van bestuur zou vormen. Ook dit staat letterlijk in de verantwoording: er is geen toegang tot de DAM-fiches via de wet van

le fait que "tous les soldes des comptes bancaires figurent dans le PCC". Il ne s'agit donc pas d'un élément nouveau. Selon le ministre, la mémoire de certains membres de la commission est très sélective. Cette décision a été prise par le gouvernement précédent et date de 2020.

Le ministre explique ensuite les modifications apportées par le projet de loi à l'examen, qui, conformément à l'accord de gouvernement, vise à créer un cadre légal régissant l'application de l'exploration de données aux données pseudonymisées du PCC en vue de la sélection de dossiers.

Alors qu'auparavant, un fonctionnaire chevronné sélectionnait, sur la base de son expérience, les dossiers à examiner plus en détail en parcourant les fichiers, cette sélection se fera désormais aussi au moyen de l'exploration anonyme de données.

En outre, le projet de loi à l'examen prévoit que les compte-titres et les comptes contenant des cryptomonnaies devront être déclarés individuellement au PCC.

— *En ce qui concerne les observations relatives à la vie privée*

Le ministre renvoie aux garanties prévues par la loi du 3 août 2012 pour les contribuables en matière de traitement des données. Le ministre souligne que ces dispositions ne sont pas modifiées d'un iota.

Il souligne également que les données ne seront utilisées qu'à des fins d'analyses de risques plus efficaces et de sélection efficace des dossiers. Ces analyses de risques seront soumises pour avis à un délégué à la protection des données (*Data Protection Officer*) dans la fiche "DAM".

La fiche DAM est utilisée pour documenter le projet spécifique d'exploration des données. Elle définit le projet, son objectif, les bases de données qui seront consultées et les explorateurs de données qui y auront accès. Elle permet de vérifier le fondement juridique et d'évaluer la proportionnalité de l'utilisation des données. Elle permet donc au SPF Finances de respecter ses obligations en matière de RGPD.

Cette fiche DAM contient les paramètres visant les infractions à la législation fiscale. Comme le ministre l'a déjà indiqué précédemment, ces paramètres s'inscrivent dans le cadre de la stratégie interne du SPF Finances.

Le ministre évoque ensuite l'observation selon laquelle les fiches DAM constitueraient une violation de la publicité de l'administration. On peut également le lire littéralement dans l'exposé des motifs: les fiches DAM

11 april 1994 betreffende openbaarheid van bestuur. Deze DAM-fiches vallen onder de uitzondering van artikel 6, § 1, 6° van dezelfde wet die voorziet in de bescherming van een federaal financieel belang, en moeten dus niet openbaar worden gemaakt. Het feit dat dat niet openbaar is, daar is niets nieuws aan, dat was in de vorige legislaturen ook al zo. Dat is altijd al zo geweest dus daar wijzigt niets aan.

Niettemin zal de minister de mogelijkheid geven om zo'n DAM-fiche hier vandaag in te kijken via de procedure "eyes only" (het gaat om een vertrouwelijk document waardoor er dus geen foto's of kopies mogen worden gemaakt).

De minister vult aan dat de ambtenaren gebonden zijn aan de strikte procedures van de fiscale wetboeken en de gegevens van de risicoanalyse niet mogen gebruiken. Dit staat letterlijk in de wettekst en in de verantwoording. De minister citeert: "De concrete gegevens afkomstig van het Centraal Aanspreekpunt mogen niet gecommuniceerd worden aan de ambtenaar bevoegd om de controle uit te voeren." (zie amendement nr. 16 van de regering, DOC 56 0963/005, p. 12).

Wat betreft de vraag naar de interpretatie van art. 322 van het WIB92 antwoordt de minister dat de verantwoording zijn inziens duidelijk is. Ook ambtenaren belast met de controle moeten hun eigen procedure volgen om de CAP-gegevens te verkrijgen. Dit geldt ook in geval van anonieme datamining. Artikel 322 van het WIB92 staat niet buiten spel en enkel ambtenaren met de nodige functieprofielen zullen de CAP-gegevens kunnen inkijken. Ook hier verandert niets, dat is vandaag al het geval.

De raadplegingsprocedure in art. 322 van het WIB92 is strikt geregeld en werkt met een getrapte procedure. De minister herhaalt wat hij reeds tijdens de eerste lezing heeft gezegd: deze procedure blijft ongewijzigd bestaan.

— De anonieme datamining zelf

De minister herhaalt dat er geen gebruik wordt gemaakt van artificiële intelligentie (AI) en dat er altijd een menselijke tussenkomst is. Ook de modules van SAS 9.4 die de administratie gebruikt, bevatten geen AI, zoals bevestigd door de FOD Financiën.

Deze toegang wordt verleend door de medewerkers die binnen elke administratie verantwoordelijk zijn voor het toegangsbeheer – wat een bijkomende controle

ne peuvent pas être consultées en vertu de la loi du 11 avril 1994 relative à la publicité de l'administration. Ces fiches DAM relèvent en effet de l'exception prévue à l'article 6, § 1^{er}, 6°, de cette même loi, qui prévoit la protection d'un intérêt financier fédéral, et ne doivent donc pas être rendues publiques. Le fait qu'elles ne soient pas publiques n'a rien de nouveau puisque c'était déjà le cas sous la législature précédente. Cela a toujours été le cas, et rien ne changera donc à cet égard.

Néanmoins, le ministre permettra aux membres de consulter, séance tenante, l'une de ces fiches DAM dans le cadre de la procédure "eyes only" (puisque'il s'agit d'un document confidentiel, il leur sera interdit de la prendre en photo ou d'en lever des copies).

Le ministre ajoute que les fonctionnaires sont tenus de respecter les procédures strictes des codes fiscaux et ne peuvent pas utiliser les données de l'analyse des risques. Cette interdiction est littéralement inscrite dans le texte de loi et dans la justification. Le ministre cite le passage en question: "Les données concrètes provenant du Point de contact central ne peuvent pas être communiquées au fonctionnaire compétent pour effectuer le contrôle" (voir l'amendement n° 16 du gouvernement, DOC 56 0963/005, p. 12).

En réponse à la question sur l'interprétation de l'article 322 du CIR92, le ministre indique que, selon lui, l'exposé des motifs est clair. Les fonctionnaires chargés du contrôle doivent également suivre leur propre procédure pour obtenir les données du PCC. Il en ira de même pour l'exploration anonyme de données. L'article 322 du CIR92 ne sera pas enfreint et seuls les fonctionnaires titulaires des profils de fonction nécessaires pourront consulter les données du PCC. Une nouvelle fois, rien ne changera à la situation actuelle.

La procédure de consultation prévue à l'article 322 du CIR92 est strictement réglementée et s'appuie sur une procédure par paliers. Le ministre répète ce qu'il a déjà indiqué lors de la première lecture: cette procédure demeurera inchangée.

— L'exploration anonyme de données à proprement parlé

Le ministre répète qu'aucune forme d'intelligence artificielle (IA) ne sera utilisée et qu'une intervention humaine sera toujours prévue. Les modules SAS 9.4 utilisés par l'administration ne contiennent pas non plus d'IA, comme l'a confirmé le SPF Finances.

Cet accès sera accordé par les collaborateurs chargés de la gestion des accès au sein de chaque administration, ce qui permettra un contrôle supplémentaire,

mogelijk maakt- overeenkomstig het ICT-principe van *Identity and Access Management*. Hierdoor is er een auditeerbare historiek van alle persoonlijke toegangen mogelijk.

— *Uitvoeringsbesluiten en KB's*

Uiteraard kunnen er maar uitvoeringsbesluiten genomen worden als er effectief een goedgekeurde wet is.

— *Wat betreft de adviezen:*

De minister merkt op dat er foutief werd geciteerd uit adviezen. Er werd hier gesteld dat de Raad van State vroeg om het advies van de NBB en de ECB te vragen.

De minister benadrukt dat dat niet klopt. De passage die werd aangehaald is nr. 3 van het advies van de Raad van State maar dit gaat niet over de artikelen 95/1, 95/2 en 95/3 van het wetsontwerp inzake anonieme datamining op het CAP. Het advies van de ECB en de NBB was niet nodig met betrekking tot de artikelen 95/1, 95/2 en 95/3 zijnde de artikelen van het CAP en anonieme datamining.

Dit staat in randnummers 3 en 4 van het advies nr. 77.807 van de Raad van State vermeld (DOC 56 0963/005, p; 35-37) waarin wordt verwezen naar de amendementen 6 tot 11 ofwel artikel 95/4 en volgende van de voorliggende wet.

De toegang tot het CAP met het oog op het uitvoeren van gerichte controles op basis van risico-indicatoren ("de anonieme datamining") wordt in artikel 95/3 vermeld.

Met betrekking tot de opmerking van de Raad van State over de verschillende adviezen van de ECB, de NBB met betrekking tot hoofdstuk 5 en de artikelen 95/4 t.e.m. 95/8 meldt de minister dat ook wanneer het uitsluitend gaat om de omzetting in nationaal recht van verplichtingen in het kader van de 6^e AML-richtlijn, zoals bedoeld in artikel 16 van de 6^e AML-richtlijn, een advies van de ECB niet noodzakelijk is, daar de ECB zich reeds heeft uitgesproken in een advies betreffende deze 6de AML-richtlijn.

Het advies van de ECB over de aanvullende bepalingen die zich niet in de 6de AML-richtlijn bevinden (zoals de mededeling van de saldi van effecten- en cryptorekeningen) werd reeds gevraagd. Op grond van gelijkaardige precedenten wordt evenwel verwacht dat de ECB zal beslissen van een beslissing af te zien daar het wetsontwerp slechts marginaal raakt aan de bevoegdheidsgebieden van de ECB.

conformément au principe informatique de gestion des identités et des accès. Cette méthode permet de disposer d'un historique vérifiable de tous les accès individuels.

— *Arrêtés d'exécution et arrêtés royaux*

Des arrêtés d'exécution ne pourront bien entendu être pris que si le projet de loi est effectivement adopté.

— *Observations concernant les avis:*

Le ministre fait observer que les avis ont parfois été cités abusivement, d'aucuns ayant soutenu que le Conseil d'État avait demandé l'avis de la BNB et de la BCE.

Le ministre souligne qu'il n'en est rien. Le passage évoqué est le point 3 de l'avis du Conseil d'État, mais celui-ci ne concerne pas les articles 95/1, 95/2 et 95/3 en projet relatifs à l'exploitation du PCC à des fins de *data mining* anonyme. Il n'était pas nécessaire de recueillir les avis de la BCE et de la BNB concernant les articles 95/1, 95/2 et 95/3, qui visent à encadrer le PCC et le *data mining* anonyme.

Cette information figure aux points 3 et 4 de l'avis n° 77.807 du Conseil d'État (DOC 56 0963/005, p. 35-37), qui renvoient aux amendements n^{os} 6 à 11, soit aux articles 95/4 et suivants du projet de loi à l'examen.

L'accès au PCC en vue de mener des contrôles ciblés sur la base d'indicateurs de risque ("le *data mining* anonyme") est prévu à l'article 95/3.

S'agissant de l'observation du Conseil d'État relative aux différents avis de la BCE et de la BNB concernant le chapitre 5 et les articles 95/4 à 95/8, le ministre indique que même lorsque les dispositions concernées visent exclusivement à transposer en droit national des obligations découlant de la sixième directive anti-blanchiment (visées en son article 16), il n'est pas nécessaire de recueillir l'avis de la BCE, dès lors que celle-ci a déjà rendu un avis sur la directive précitée.

L'avis de la BCE sur les dispositions additionnelles qui ne figurent pas dans la sixième directive anti-blanchiment (telles que la communication des soldes des comptes-titres et des comptes de cryptomonnaies) a déjà été demandé. On s'attend toutefois, sur la base de précédents similaires, à ce que la BCE décide de renoncer à cet avis, dès lors que le projet de loi à l'examen n'affecte que marginalement ses domaines de compétence.

Wat betreft de NBB, die is uiteraard als operator en beheerder geconsulteerd bij de werkzaamheden van de totstandkoming van deze wetteksten, gelet op haar expertise ter zake. Dat is nogal logisch want de NBB was eveneens betrokken en geconsulteerd bij het ontwerp van de AML-richtlijn. Zij zou dan een advies geven over haar eigen inbreng.

De inspecteur van Financiën gaf zijn advies over alle bepalingen opgenomen in de oorspronkelijke programwet. Ook de inspecteur van Financiën beschikte dus over alle teksten terzake. Nadien is de programwet opgesplitst in een deel dat al werd goedgekeurd in het Parlement en een deel diverse fiscale bepalingen dat nu ter bespreking voorligt ten gevolge van opmerkingen van de Raad van State. De teksten van het CAP zaten dus reeds in de oorspronkelijke programwet. De teksten van het CAP zijn op meerdere interkabinettenwerkgroepen (IKW's) en ook verschillende keren op de Ministerraad besproken en goedgekeurd.

De minister is van mening dat het intentieproces dat hiervan door sommige commissieleden werd gemaakt in deze commissie, dus kant noch wal raakt.

— *Andere vragen:*

Wat betreft de vraag inzake art. 333/1, § 2, laatste lid, van het WIB92, antwoordt de minister dat dat in deze geheel irrelevant is. De verschillende wetsbepalingen waarnaar in deze paragraaf wordt verwezen, zijn dan ook niet door deze amendementen en door deze wet diverse bepalingen aangepast.

Niettemin heeft de minister aan zijn administratie gevraagd of dit rapport werd opgemaakt en bezorgd aan het Parlement. Dat is blijkbaar al sinds 2015 niet meer het geval.

Er werd gevraagd of de banken verplicht zullen worden om te melden dat er met het oog op dossierselectie anonieme datamining zal worden toegepast: het antwoord is negatief. De mededeling aan de cliënteel bepaald door artikel 5, § 1, van de CAP-Wet volstaat.

— *Er werd gevraagd of iemand kan raadplegen of de gegevens zijn ingekeken:*

De minister verwijst naar artikel 8, § 1, van wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt. In haar hoedanigheid van verantwoordelijke voor de verwerking registreert de NBB alle aanvragen om informatie van het CAP die door de centraliserende organisaties of, bij gebrek hiervan, door de informatie-gerechtigden worden ingediend, teneinde de uitoefening

En ce qui concerne la BNB, elle a bien entendu été consultée en sa qualité d'opérateur et de gestionnaire lors du processus d'élaboration des textes législatifs à l'examen, compte tenu de son expertise en la matière. C'est d'ailleurs plutôt logique, puisque la BNB avait également été associée et consultée lors de l'élaboration de la directive anti-blanchiment. Elle avait alors dû rendre un avis sur sa propre contribution.

L'inspecteur des finances a, quant à lui, rendu un avis sur toutes les dispositions inscrites initialement dans la loi-programme. Il disposait donc lui aussi de l'ensemble des textes. La loi-programme a par la suite été scindée en deux parties à la suite des observations formulées par le Conseil d'État: une partie déjà adoptée au Parlement et une partie portant des dispositions fiscales diverses, qui fait l'objet de la présente discussion. Les textes relatifs au PCC figuraient donc déjà dans la loi-programme initiale. Ils ont été examinés à plusieurs reprises par les groupes de travail intercabinets ainsi que par le Conseil des ministres avant d'être approuvés.

Le ministre estime que le procès d'intention auquel se sont livrés certains membres en commission ne rime donc à rien.

— *Autres questions:*

En réponse à la question relative à l'article 333/1, § 2, dernier alinéa, du CIR 92, le ministre indique que cette question est dénuée de toute pertinence. Les différentes dispositions législatives auxquelles renvoie ce paragraphe ne sont en effet modifiées ni par le projet de loi à l'examen, ni par les amendements.

Le ministre a néanmoins demandé à son administration si ce rapport avait été établi et transmis au Parlement. Apparemment, ce n'est déjà plus le cas depuis 2015.

Il a été demandé si les banques seraient tenues de signaler le recours au *data mining* anonyme aux fins de la sélection des dossiers. Le ministre répond par la négative. La communication à la clientèle prévue à l'article 5, § 1^{er}, de la loi relative au PCC suffira.

— *Est-il possible de vérifier si les données du PCC ont été consultées?:*

En réponse à cette question, le ministre renvoie à l'article 8, § 1^{er}, de la loi du 8 juillet 2018 portant organisation d'un point de contact central. En sa qualité de responsable du traitement, la BNB enregistre toutes les demandes d'information du PCC introduites par les organisations centralisatrices ou, à défaut, par les personnes habilitées à recevoir l'information, en vue de garantir

te garanderen van het recht van inzage van de persoon waarop deze informatie slaat, zoals bepaald door artikel 15 van voornoemde Verordening (EU) 2016/679 van 27 april 2016. De NBB bewaart de lijst van de aanvragen om informatie van het CAP gedurende twee kalenderjaren.

— *Er werden allerhande gegevens en bedragen gevraagd:*

De minister merkt vooreerst dat het stellen van een schriftelijke vraag daarvoor meer aangewezen is. De minister benadrukt dat hij, samen met de beleidscel en de administratie snel en correct tracht te antwoorden op alle vragen.

De FOD Financiën betaalde volgende bedragen voor de consultatie van het CAP: in 2022 ongeveer 1 miljoen euro, in 2023 ongeveer 906.000 euro en in 2024 ongeveer 885.000 euro.

Wat betreft de vraag wie verantwoordelijk is voor de gegevensbescherming en de veiligheid van het systeem antwoordt de minister dat de NBB daar zelf voor verantwoordelijk is.

Vervolgens werd bijna letterlijk een FAQ voorgelezen van 34 pagina's die online beschikbaar is. De minister kan bevestigen dat alles wat daarin staat correct is en dat elke belastingplichtige deze informatie transparant kan terugvinden op de website van de Nationale Bank. Hij kan daar weinig aan toevoegen.

Ook ganse bepalingen uit de wet van 8 juli 2018 werden voorgelezen. Ook daar kan de minister weinig aan toevoegen.

Wat betreft de vragen inzake termijnrekeningen, effectenrekeningen, betaalrekeningen, kredietkaarten, etc. antwoordt de minister dat alle gegevens die nu al opgenomen zijn in het Centraal Aanspreekpunt inderdaad onder de anonieme datamining zullen vallen. Ook dat staat letterlijk in de huidige bepalingen.

Wat betreft de opmerking inzake de effectenrekeningen verwijst de minister naar de verantwoording bij het nieuwe art. 95/6 van het WIB92. Daarin wordt duidelijk vermeld dat het periodieke saldo moet worden meege-deeld, wat tot nu toe nog niet het geval is.

— *Wat betreft vragen over de adviezen van de GBA:*

l'exercice du droit d'accès de la personne sur laquelle porte cette information, tel que prévu par l'article 15 du règlement (UE) 2016/679 du 27 avril 2016 précité. La BNB conserve la liste des demandes d'information du PCC pendant deux années civiles.

— *Demande de toutes sortes de données et de montants:*

Le ministre tient d'abord à souligner qu'il est préférable de poser une question écrite à ce sujet. Il ajoute qu'il s'efforce, en collaboration avec la cellule stratégique et l'administration, de répondre rapidement et correctement à toutes les questions.

Le SPF Finances a versé les sommes suivantes pour la consultation du PCC: environ 1 million d'euros en 2022, environ 906.000 euros en 2023 et environ 885.000 euros en 2024.

En ce qui concerne la question de savoir qui est responsable de la protection des données et de la sécurité du système, le ministre répond que c'est la BNB elle-même qui en est responsable.

Le ministre indique ensuite qu'un membre a quasiment lu mot à mot une FAQ de 34 pages disponible en ligne. Il peut confirmer que tout ce qui y figure est correct et que chaque contribuable peut consulter ces informations en toute transparence sur le site de la Banque nationale. Il ne peut guère en dire plus.

Des dispositions entières de la loi du 8 juillet 2018 ont également été citées. Une fois encore, le ministre ne peut guère en dire plus.

En ce qui concerne les questions relatives aux comptes à terme, aux comptes-titres, aux comptes de paiement, aux cartes de crédit, etc., le ministre répond que toutes les données déjà enregistrées dans le Point de contact central seront en effet soumises au *data mining* anonyme, comme le prévoient d'ailleurs expressément les dispositions actuelles.

S'agissant de l'observation relative aux comptes-titres, le ministre renvoie à la justification relative au nouvel article 95/6 du CIR 92. Il y est clairement indiqué que le solde périodique devra être communiqué, ce qui n'était pas le cas jusqu'à présent.

— *En ce qui concerne les questions relatives aux avis de l'APD:*

Alle adviezen zijn gewoon transparant en openbaar terug te vinden op de website van de GBA. Ook die over het CAP. Daar is dus helemaal niets geheimzinnig aan.

— *Wat betreft de vragen over de bewaartermijnen:*

Artikel 95/3 van het wetsontwerp voegt in artikel 5, § 3, tweede lid van de wet van 3 augustus 2012 een duidelijke bewaartermijn toe. Voor de volledigheid citeert de minister het betreffende lid: “Onverminderd de bewaring noodzakelijk voor de verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden bedoeld in artikel 89 van de algemene verordening gegevensbescherming, worden de persoonsgegevens die voortkomen uit de verwerkingen in het datawarehouse niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor zij werden verwerkt, met een maximale bewaartermijn die één jaar na de verjaring van alle vorderingen die tot de bevoegdheid van de verwerkingsverantwoordelijke behoren en, in voorkomend geval, de definitieve beëindiging van de administratieve en rechterlijke procedures en rechtsmiddelen en de integrale betaling van alle hiermee verbonden bedragen niet mag overschrijden.”

De minister besluit hieruit dat er dus duidelijk een maximale en proportionele bewaartermijn wordt vermeld.

— *Voor de vragen inzake de “data protection impact assessments”:*

De *Data Protection Impact Assessments* zijn inderdaad opgesteld en beschikbaar voor de GBA. Deze zijn ook raadpleegbaar ingevolge de Wet Openbaarheid van Bestuur van 11 april 1994.

De juridische basis is artikel 6.1.e van de Algemene Verordening Gegevensbescherming (AVG). Hierin staat vermeld dat de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust. In casu is de FOD Financiën als verwerkingsverantwoordelijke belast met een dergelijke wettelijke verplichting namelijk de vestiging en inning van belasting, een taak van algemeen belang.

— *Wat betreft de Informatieplicht:*

De NBB en de FOD Financiën moeten op hun website meedelen dat de gegevens aan de FOD Financiën worden overgemaakt en voor welke doeleinden die gebruikt worden, met inbegrip van de modaliteiten van de anonieme datamining.

Tous les avis sont absolument transparents et accessibles au public sur le site web de l'APD, y compris ceux concernant le PCC. Ces avis ne sont donc en aucun cas secrets.

— *En ce qui concerne les questions relatives à la durée de conservation:*

L'article 95/3 du projet de loi insère une durée de conservation claire à l'article 5, § 3, alinéa 2, de la loi du 3 août 2012. Dans un souci d'exhaustivité, le ministre cite l'alinéa concerné: “Sans préjudice de la conservation nécessaire pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques visé à l'article 89 du règlement général sur la protection des données, les données à caractère personnel qui résultent des traitements dans le datawarehouse ne sont pas conservées plus longtemps que nécessaire au regard des finalités pour lesquelles elles sont traitées, avec une durée maximale de conservation ne pouvant excéder un an après la prescription de toutes les actions qui relèvent de la compétence du responsable du traitement et, le cas échéant, la cessation définitive des procédures et recours administratifs et judiciaires ainsi que du paiement intégral de tous les montants y liés.”

Le ministre en conclut qu'une durée de conservation maximale et proportionnée est clairement prévue.

— *En ce qui concerne les questions liées aux analyses d'impact relatives à la protection des données:*

Ces analyses ont effectivement été réalisées et mises à la disposition de l'APD. Elles sont également consultables conformément à la loi relative à la publicité de l'administration du 11 avril 1994.

L'article 6, 1., e), du règlement général sur la protection des données (RGPD) en constitue le fondement juridique. Conformément à cette disposition, le traitement est licite s'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. En l'espèce, le SPF Finances, en tant que responsable du traitement, est légalement chargé d'une mission d'intérêt public, à savoir l'établissement et la perception des impôts.

— *En ce qui concerne l'obligation d'information:*

La BNB et le SPF Finances doivent signaler en ligne que les données sont transmises au SPF et en préciser les finalités, y compris les modalités du *data mining* anonyme.

Tot slot is het openbaar voor alle belastingplichtigen dat de FOD Financiën de gegevens van het CAP ontvangt en dat deze mogelijks kunnen worden gebruikt voor anonieme datamining en dossierselectie. Dit werd treffend bewezen met het volledig citeren van de publieke FAQ die online beschikbaar is.

Inzake het EVRM en het Handvest van de grondrechten van de Europese Unie is de minister ervan overtuigd dat de artikelen in het huidige wetsontwerp geen problemen stelt.

De minister verwijst daarvoor naar het arrest van het Grondwettelijk Hof van 2022 (Arrest nr. 162/2022 van 8 december 2022). In dat arrest werd het beroep verworpen. Het Hof oordeelde dat de uitbreiding van de gegevens beantwoordt aan wat men noemt een “dringende maatschappelijke behoefte”.

En, zoals aangegeven in artikel 5, § 3, zesde lid, van de wet 3 augustus 2012, wordt duidelijk gesteld dat deze bescherming van het EVRM evengoed rust op dergelijke gegevens. De in het bovenvermelde arrest vermelde waarborgen blijven onverkort van toepassing.

In de overweging B12 van het arrest staat het volgende te lezen: “De bestreden artikelen schenden niet artikel 22 van de Grondwet, in samenhang gelezen met artikel 8 van het Europees Verdrag voor de rechten van de mens, met de artikelen 7, 8 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, met artikel 16, lid 1, van het Verdrag betreffende de werking van de Europese Unie en met artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten.”

Daarnaast oordeelt het Hof dat de uitbreiding van de gegevens die moeten worden meegedeeld beantwoordt aan een dwingende maatschappelijke behoefte in een democratische samenleving. Die uitbreiding verhoogt de transparantie op fiscaal niveau en maakt het mogelijk om op efficiënte wijze en tegen lagere kosten belastingfraude te bestrijden.

De raadplegingsprocedure voor fiscale ambtenaren vervolgens is strikt omkaderd, om oneigenlijk gebruik van de geraadpleegde gegevens te vermijden.

Zo kan de bevoegde ambtenaar de gegevens slechts raadplegen wanneer hij beschikt over één of meer aanwijzingen van belastingontduiking en moet de belastingplichtige ervan op de hoogte worden gebracht. Ten slotte zijn alle betrokkenen onderworpen aan een geheimhoudingsplicht.

Enfin, tous les contribuables savent que le SPF Finances reçoit les données du PCC et que celles-ci peuvent être utilisées, le cas échéant, à des fins de *data mining* anonyme et de sélection de dossiers, comme l'indique clairement la lecture de la FAQ publique consultable en ligne.

En ce qui concerne la CEDH et la Charte des droits fondamentaux de l'Union européenne, le ministre est convaincu que les articles du projet de loi actuel ne posent aucun problème.

Le ministre renvoie à cet égard à l'arrêt de la Cour constitutionnelle de 2022 (arrêt n° 162/2022 du 8 décembre 2022) qui a rejeté le recours visé, estimant que l'extension des données répondait à un “besoin social impérieux”.

De plus, comme l'indique clairement l'article 5, § 3, alinéa 6, de la loi du 3 août 2012, la protection accordée par la CEDH repose également sur ces données. Les garanties énoncées dans l'arrêt susmentionné restent intégralement applicables.

Le considérant B.12. de l'arrêt indique ce qui suit: “Les articles attaqués ne violent pas l'article 22 de la Constitution, lu en combinaison avec l'article 8 de la Convention européenne des droits de l'homme, avec les articles 7, 8 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, avec l'article 16, paragraphe 1, du Traité sur le fonctionnement de l'Union européenne et avec l'article 17 du Pacte international relatif aux droits civils et politiques.”

En outre, la Cour estime que l'extension des données devant être communiquées répond à un besoin social impérieux dans une société démocratique. Cette extension créera une plus grande transparence au niveau fiscal et permettra également de lutter efficacement et à moindre coût contre la fraude fiscale.

Ensuite, la procédure de consultation pour les agents fiscaux demeurera encadrée de manière stricte pour éviter tout usage inapproprié des données consultées.

L'agent compétent pourra consulter les données, uniquement lorsqu'il disposera d'un indice ou de plusieurs indices de fraude fiscale. Il devra également en informer le contribuable. Enfin, toutes les personnes concernées seront soumises à une obligation de secret.

De minister verwijst ook naar zijn uitgebreide antwoorden in de eerste lezing. Ter bescherming van de rechten van iedere in het CAP geregistreerde persoon wordt bovendien voorzien in een geheimhoudingsplicht voor alle informatiegerechtigden en centraliserende organisaties (artikel 8, § 2, 4°, en § 4, 4°, van de CAP-Wet).

Volgens het Grondwettelijk Hof vormen die procedurele en inhoudelijke vereisten belangrijke waarborgen tegen willekeurige inmengingen in het privéleven van de betrokken personen. Ook daar is geen wijziging.

Het Hof komt dan ook tot het besluit dat de uitbreiding van de meldingsplichtige gegevens het recht op de bescherming van het privéleven van de betrokken personen niet schendt.

Ook nu streven de bepalingen inzake het CAP een doel van algemeen belang na in de zin van art. 8.2. van het Europees Verdrag voor de Rechten van de Mens, in zoverre de doeltreffende invordering van de belasting ertoe strekt de gelijkheid van de burgers voor de fiscale wet te waarborgen. Er zijn nog steeds voldoende procedurele en inhoudelijke waarborgen ingebouwd tegen willekeurige inmengingen in het privéleven.

— *Wat betreft de vragen over mogelijke klachten en bezwaren:*

Een belastingplichtige kan steeds terecht bij de GBA voor een informatieverzoek, bemiddelingsverzoek of een klacht.

Elke belastingplichtige kan ook steeds een bezwaar indienen als hij het niet eens is met een beslissing van de FOD Financiën.

Met ingang van de inwerkingtreding van wet van 2 december 2021 zijn ook informatiegerechtigden verplicht om de Administratie van de Thesaurie op de hoogte te brengen van het bestaan van foutieve of ontbrekende gegevens in de informatie die ze ontvangen van het CAP.

Met betrekking tot de verplichting voor de bevoegde personen om ontbrekende of foutieve gegevens in hoofde van het CAP mee te delen aan de Algemene Administratie van de Thesaurie krachtens artikel 13 § 1, derde lid, van de CAP-wet, kan de minister de volgende gegevens meedelen:

Le ministre renvoie également aux réponses détaillées qu'il a données en première lecture. À des fins de protection des droits de toute personne enregistrée dans le PCC, le législateur a en outre prévu une obligation de secret pour toutes les personnes habilitées à recevoir l'information et organisations centralisatrices (article 8, § 2, 4°, et § 4, 4°, de la loi relative au PCC).

Selon la Cour constitutionnelle, toutes ces conditions procédurales et concrètes constituent des garanties importantes contre des ingérences arbitraires dans la vie privée des personnes concernées. Là encore, aucun changement n'est apporté.

La Cour conclut dès lors en indiquant que l'extension des données soumises à l'obligation de déclaration ne portera pas atteinte au droit à la protection de la vie privée des personnes concernées.

Aujourd'hui encore, les dispositions relatives au PCC poursuivent un objectif d'intérêt général au sens de l'article 8.2., de la Convention européenne des droits de l'homme, dans la mesure où le recouvrement efficace de l'impôt vise à garantir l'égalité des citoyens devant la loi fiscale. Il existe toujours suffisamment de garanties procédurales et concrètes contre les ingérences arbitraires dans la vie privée.

— *En ce qui concerne les questions relatives aux plaintes et aux réclamations éventuelles:*

Tout contribuable peut toujours s'adresser à l'APD pour demander des informations, demander une médiation ou porter plainte.

Tout contribuable peut également faire opposition lorsqu'il n'est pas d'accord avec une décision du SPF Finances.

Depuis l'entrée en vigueur de la loi du 2 décembre 2021, les personnes habilitées à recevoir l'information qui constatent l'existence de données erronées ou manquantes dans l'information qu'elles reçoivent du PCC sont également tenues de les communiquer à l'Administration de la Trésorerie.

En ce qui concerne l'obligation incombant aux personnes compétentes de communiquer à l'Administration générale de la Trésorerie les données manquantes ou erronées reçues du PCC en vertu de l'article 13, § 1^{er}, alinéa 3, de la loi relative au PCC, le ministre est en mesure de donner les réponses exposées ci-dessous aux questions suivantes:

— Hoe vaak is dit gebeurd? Behoudens vergissing of weglating, heeft de FOD Financiën voor 2024 19 meldingen ontvangen, voor 2025, 27 meldingen.

— Welke bevoegde personen die de informatie mogen ontvangen, hebben deze meldingen gedaan? Het gaat hoofdzakelijk om de gerechtelijke politie en het parket voor de problematiek van virtuele IBAN's, de niet-vermelding van rijksregisternummers of KBO-nummers.

— Hoe vaak werd een sanctie opgelegd door de Thesaurie? Er werd geen enkele sanctie opgelegd omdat er telkens een rechtvaardiging was.

— Wie waren de betrokken informatieplichtigen? Het gaat hoofdzakelijk om betalingsinstellingen.

— *Wat betreft de vragen over de aansprakelijkheid:*

Volgens artikel 83 van de AVG worden inbreuken op de verplichtingen van de verwerkingsverantwoordelijke en de verwerker krachtens de artikelen 37, 38 en 39 met betrekking tot de functionaris voor gegevensbescherming onderworpen aan administratieve geldboeten tot 10.000.000 euro of, voor een onderneming, tot 2 % van de totale wereldwijde omzet van het voorgaande boekjaar, indien dit bedrag hoger is. Indien de contactgegevens van de functionaris niet aan de betrokkenen worden meegedeeld (artikelen 13 en 14 van de AVG), wordt het plafond van deze administratieve geldboeten verhoogd tot 20.000.000 euro of 4 % van de totale wereldwijde omzet van het voorgaande boekjaar.

In het algemeen zijn deze administratieve geldboeten niet de enige vorm van administratieve sancties die door gegevensbeschermingsautoriteiten kunnen worden opgelegd. Er staan de gegevensbeschermingsautoriteit andere maatregelen ter beschikking bij de uitoefening van haar corrigerende bevoegdheden (artikel 58, lid 2 van de AVG) zoals bijvoorbeeld een waarschuwing, een berisping en een bevel tot het in overeenstemming brengen van de verwerking. Wanneer de Gegevensbeschermingsautoriteit administratieve sancties oplegt, houdt zij rekening met de context, de feiten en de stukken van het dossier. Ter zake wordt ook verwezen naar de artikelen 222-230 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

— *Wat betreft de vele vragen en opmerkingen over de Nederlandse toeslagenaffaire:*

— Combien de fois cela s'est-il produit? Sauf erreur ou omission, le SPF Finances a reçu 19 signalements pour 2024 et 27 signalements pour 2025.

— Quelles sont les personnes compétentes habilitées à recevoir ces informations qui ont fait ces signalements? Il s'agit principalement de la police judiciaire et du parquet en ce qui concerne les IBAN virtuels et la non-communication de numéros de registre national ou de numéros de la BCE.

— À combien de reprises une sanction a-t-elle été infligée par la Trésorerie? Aucune sanction n'a été infligée, car une justification a systématiquement été donnée.

— Qui étaient les personnes habilitées à recevoir l'information? Il s'agissait principalement d'établissements de paiement.

— *En ce qui concerne les questions relatives à la responsabilité:*

Conformément à l'article 83 du RGPD, les violations des obligations incombant au responsable du traitement et au sous-traitant en vertu des articles 37, 38 et 39 en ce qui concerne le délégué à la protection des données sont passibles d'amendes administratives pouvant atteindre 10.000.000 euros ou, dans le cas d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, si ce montant est le plus élevé. Si les coordonnées du délégué ne sont pas communiquées aux personnes concernées (articles 13 et 14 du RGPD), le plafond de ces amendes administratives est porté à 20.000 00 euros ou 4 % du chiffre d'affaires mondial total de l'exercice précédent.

En général, ces amendes administratives ne sont pas les seules sanctions administratives qui peuvent être infligées par les autorités chargées de la protection des données. Ces autorités disposent en effet d'autres possibilités dans le cadre de l'exercice de leurs compétences correctrices (article 58, 2, du RGPD): avertissement, rappel à l'ordre et ordre de mettre les opérations de traitement en conformité. Lorsque l'Autorité de protection des données inflige des sanctions administratives, elle tient compte du contexte, des faits et des pièces du dossier. À cet égard, il est également renvoyé aux articles 222 à 230 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

— *En ce qui concerne les nombreuses questions et observations relatives à l'"affaire des allocations" aux Pays-Bas:*

Het gaat bij datamining op de gegevens uit het CAP niet om een volledig geautomatiseerde beslissing zoals in Nederland. Er zijn voldoende waarborgen voorzien, zoals de minister reeds heeft aangehaald. De minister verwijst nogmaals naar de *Data Protection Impact Assessments*. Ook hierover heeft de minister het reeds uitgebreid gehad in de eerste lezing.

In Nederland gebruikte de belastingdienst geautomatiseerde checks waardoor bepaalde aanvragen automatisch geblokkeerd werden. Maar, zoals in de antwoorden op de schriftelijke vragen van Mr. Mathei te lezen is: “elk selectiemechanisme is afhankelijk van een menselijke tussenkomst”. De minister benadrukt opnieuw dat daar niets aan wijzigt.

— *Wat betreft de vraag naar de menselijke tussenkomst*

De selectie zelf, is in geen geval een bewijs van fiscale fraude. Dit staat in de zevende paragraaf van het artikel 95/3. Er is dus geen vermoeden van schuld. Het vermoeden van onschuld wordt niet afgeschaft.

Wanneer een dossier wordt geselecteerd in het kader van datamining, wordt dit behandeld als iedere andere controle. Hieromtrent worden er dan ook geen afzonderlijke regels voorzien.

— *Er werd vorige keer gesteld dat vanaf nu “iedereen fraudeur is tot het tegendeel bewezen is”*

Het moet gaan om het “plegen van een inbreuk op een wet”. Dat staat zwart op wit in de verantwoording van de wetbepalingen.

De minister onderstreept dat anonieme datamining dient om met concrete parameters mogelijke fiscale inbreuken te detecteren. Het is een manier om dossierselectie mogelijk te maken die nu manueel gebeurt. Net zoals dat vandaag al gebeurt voor andere fiscale inbreuken. Ook dit is niet nieuw. Het is een manier om op een efficiënte wijze aan fraudebestrijding te doen.

Het gaat hier dus niet over een eenvoudige storting zoals sommigen hier stellen, want dat is geen fiscale inbreuk. Er wordt niet gekeken “*in de bankapp*” zoals sommigen verkeerdelijk stellen.

Le *data mining* appliqué aux données provenant du PCC ne repose pas sur une décision entièrement automatisée, comme aux Pays-Bas. Comme le ministre l'a déjà indiqué, la législation a prévu des garanties suffisantes. Le ministre renvoie une nouvelle fois aux analyses d'impact relatives à la protection des données (AIPD), qu'il a déjà largement commentées lors de la première lecture.

Aux Pays-Bas, l'administration fiscale a appliqué des contrôles automatisés qui ont entraîné le blocage automatique de certaines demandes. Mais, comme l'indiquent les réponses aux questions écrites de M. Mathei, tout mécanisme de sélection dépend d'une intervention humaine. Le ministre répète que rien ne changera à ce niveau.

— *S'agissant de la question relative à l'intervention humaine*

La sélection en soi ne constitue en aucun cas une preuve de fraude fiscale, comme l'indique le paragraphe 7 de l'article 95/3. Il n'existe donc pas de présomption de culpabilité. La présomption d'innocence ne sera pas abolie.

Lorsqu'un dossier sera sélectionné dans le cadre du *data mining*, il sera traité comme n'importe quel autre contrôle. Aucune règle distincte n'est dès lors prévue à cet égard.

— *Il a été indiqué lors de la dernière réunion que, désormais, “tout le monde sera fraudeur jusqu'à preuve du contraire”*

Il devra s'agir de la “commission d'une infraction à une loi”, comme indiqué noir sur blanc dans la justification des dispositions légales.

Le ministre souligne que le *data mining* anonyme servira à détecter d'éventuelles infractions fiscales à l'aide de paramètres concrets. Cette technique permettra la sélection des dossiers, aujourd'hui manuelle, telle qu'elle est d'ores et déjà pratiquée pour d'autres infractions fiscales. Cela non plus n'a rien de nouveau. C'est une méthode efficace de lutte contre la fraude.

Les simples versements ne seront donc pas visés, contrairement à ce que certains prétendent au sein de cette commission, car ces opérations ne constituent pas une infraction fiscale. Les applications bancaires ne seront pas examinées, comme d'aucuns l'affirment erronément.

Een storting van cash is géén fiscale inbreuk. De hulp van je ouders voor de bouw van een keuken is geen fiscale inbreuk.

Er bestaat – althans juridisch – niet iets zoals “kleine fraude” en “grote fraude” maar er is wel een afweging tussen toegang tot de gegevens en het proportioneel gebruik van deze gegevens. Deze zit nu eenmaal verankerd in de AVG. Dit is ook in de verantwoording vermeld. Daarnet heeft de minister in zijn antwoorden ook duidelijk verwezen naar arresten van het Grondwettelijk Hof die deze proportionaliteit beamen.

Het CAP bevat de saldi die twee keer per jaar worden meegedeeld, niet alle verrichtingen of transacties op de rekeningen van de Belgen. De minister verwijst daarvoor naar de programmawet van 20 december 2020. Sommige commissieleden noemen programmawetten of een diverse wet een “vuilnisbakwet” en eisen dat het CAP als een “aparte wet” moet worden behandeld.

In een vorige legislatuur werd met zo’n “vuilnisbakwet” de financiële instellingen verplicht de halfjaarlijkse saldi van de betaalrekeningen aan het CAP te melden.

Niettemin, streeft de minister naar meer thematische wetgeving. De kritiek van sommige commissieleden hierover lijkt volgens de minister nogal inconsequent in woord en daad.

Wat de bewering betreft dat iedereen plots verdacht is en dat er geen anonimiteit is of zal zijn antwoordt de minister dat deze bewering gewoon feitelijk niet klopt. Ambtenaren zijn gebonden aan een strikt beroepsgeheim en riskeren serieuze tuchtmaatregelen wanneer ze dit schenden. De regels zijn terug te vinden in artikel 337 van het WIB92. Het niet-respecteren van bepaalde regels kan aanleiding geven tot een tuchtprocedure en eventuele tuchtstraffen waaronder afzetting.

— *Er kwam kritiek op de zogenaamde onleesbare zevende lid van de voorgestelde paragraaf 3 van de artikel 5 van de wet van 3 augustus 2012 (artikel 95/3 (nieuw) van het wetsontwerp)*

De minister citeert letterlijk de tekst van het betrokken zevende lid: De selectie van het dossier die voorkomt uit de in het eerste lid bedoelde processen – dat is dus de anonieme datamining, – vormt in geen geval een bewijs van fiscale fraude vatbaar om direct tot de

Un versement en espèces n’est pas une infraction fiscale, pas plus que l’aide apportée par des parents pour installer une nouvelle cuisine.

Il n’existe pas, du moins juridiquement, de “petite fraude” ni de “grande fraude”, mais il y a bien une mise en balance entre l’accès aux données et l’usage proportionné de ces données. Cet équilibre est tout simplement ancré dans le RGPD, et il figure également dans la justification. Le ministre vient également de renvoyer en des termes clairs, dans ses réponses, à des arrêts de la Cour constitutionnelle qui confirment cette proportionnalité.

Le PCC contient les soldes qui sont communiqués deux fois par an, et non toutes les opérations ou transactions effectuées sur les comptes des Belges. Le ministre renvoie à cet égard à la loi-programme du 20 décembre 2020. Certains membres de la commission qualifient les lois-programmes, ou une lois portant dispositions diverses, de “lois poubelles” et exigent que le PCC soit traité dans le cadre d’une “loi distincte”.

Au cours d’une législature précédente, les institutions financières ont été obligées, par la voie d’une telle “loi poubelle”, de communiquer les soldes semestriels des comptes de paiement au PCC.

Le ministre s’attèle néanmoins à une législation plus thématique. Le ministre estime que la critique émise à ce sujet par certains membres de la commission semble relativement incohérente, dans les paroles comme dans les actes.

En ce qui concerne l’affirmation selon laquelle tout le monde sera soudainement suspect et qu’il n’existera désormais plus d’anonymat, le ministre répond que les faits démentent tout simplement cette interprétation. Les fonctionnaires sont tenus par un secret professionnel strict et s’exposent à de graves mesures disciplinaires s’ils le violent. Les règles figurent à l’article 337 du CIR92. Le non-respect de certaines règles peut donner lieu à une procédure disciplinaire et à d’éventuelles sanctions disciplinaires, dont la révocation.

— *Des critiques ont été formulées au sujet du caractère prétendument illisible de l’alinéa 7 du paragraphe 3 proposé de l’article 5 de la loi du 3 août 2012 (article 95/3 (nouveau) du projet de loi)*

Le ministre cite textuellement l’alinéa 7 en question: “La sélection de dossier résultant des opérations visées à l’alinéa 1^{er} – il s’agit donc du data mining anonyme – ne constitue en aucun cas une preuve de fraude fiscale susceptible de mener directement à la taxation d’un

belastingheffing bij een bepaalde belastingplichtige te leiden en doet geen afbreuk aan de rechten die hem zijn toegekend door de fiscale regelgeving.

Die tekst lijkt dus duidelijk:

- een selectie is geen bewijs van fiscale fraude,
- kan niet leiden tot een directe belastingheffing en;
- doet geen afbreuk aan de rechten van de belastingplichtigen. Die rechten zijn gewaarborgd door de wet van 3 augustus 2012, zoals de minister reeds meerdere keren heeft gezegd. Aan die wet wordt niets gewijzigd.

De minister citeert opnieuw uit het verslag van deze commissie, (DOC 53 2343/003, p. 11). Daarin stelt een lid (mevrouw Gwendolyn Rutten) dat “sommigen altijd wantrouwig staan tegenover de instellingen, maar elke overdrijving is absurd. Het wetsontwerp betreffende de verwerking van persoonsgegevens dat hier dus van toepassing is – is evenwichtig en werkt een objectieve werking in de hand.”

De minister besluit dat er dus ook helemaal geen sprake van, zoals sommige commissieleden zeggen, van het overboord gooien van het vermoeden van onschuld of erger, van een totalitaire staat.

— *Wat betreft de opmerkingen inzake indiciaire afrekeningen van artikel 341 van het WIB92:*

Een indiciair tekort is een aanwijzing van fraude, dat is rechtspraak van het Hof van Cassatie (zie arrest van 22 april 2016), waarmee dus nogmaals wordt benadrukt dat het Centraal Aanspreekpunt en de anonieme data-mining gericht is tegen fiscale inbreuken.

Daarom wordt aan de belastingplichtige ook alle mogelijkheid gelaten om het tegenbewijs te leveren bij een indiciair tekort “De fiscus stelt zich coöperatief op als er een valabele uitleg wordt gegeven”, zei de heer Vereeck. Wel nu, dat is het concept van tegenbewijs. Er is geen wijziging aan die procedure van het indiciaire tekort. De minister benadrukt opnieuw dat er niets wordt gewijzigd. Er is dus niets nieuws.

— *Wat betreft de opmerkingen inzake artificiële intelligentie:*

AI is een zelflerend systeem enkel en alleen door computers gedreven

Het SAS-programma bevat geen AI-gedreven modules. Enkel traditionele dataminingstechnieken zullen worden gebruikt voor de CAP-gegevens zonder gebruik

contribuable déterminé et ne porte pas préjudice aux droits qui lui sont reconnus par la réglementation fiscale.”

Ce texte paraît donc clair:

- une sélection n'est pas une preuve de fraude fiscale;
- elle ne peut pas conduire à une imposition directe et;
- elle ne porte pas préjudice aux droits des contribuables. Ces droits sont garantis par la loi du 3 août 2012, comme le ministre l'a déjà indiqué à plusieurs reprises. Aucune modification n'est apportée à cette loi.

Le ministre cite de nouveau le rapport de cette commission (DOC 53 2343/003, p. 11). On peut y lire qu'une membre (Mme Gwendolyn Rutten) indique que: “Certaines personnes se méfient toujours des institutions, mais toute exagération est absurde. Le projet de loi relatif aux traitements de données à caractère personnel, qui est donc d'application en l'espèce, est équilibré et contribue à un fonctionnement objectif.”

Le ministre conclut qu'il n'est donc absolument pas non plus question de renoncer à la présomption d'innocence – voire pire, d'instaurer un État totalitaire –, contrairement à ce qu'affirment certains membres de la commission.

— *S'agissant des observations relatives aux décomptes indiciaires de l'article 341 du CIR92:*

Un déficit indiciaire est un indice de fraude, comme l'établit la jurisprudence de la Cour de cassation (voir l'arrêt du 22 avril 2016). Il est donc de nouveau souligné que le Point de contact central et le *data mining* anonyme se concentrent sur les infractions fiscales.

C'est pourquoi le contribuable conserve pleinement la possibilité d'apporter la preuve contraire en cas de déficit indiciaire. M. Vereeck a signalé que le fisc se montrait coopératif lorsqu'une explication valable était apportée. C'est le concept même de la preuve contraire. Cette procédure relative au déficit indiciaire reste inchangée. Le ministre insiste encore une fois sur ce point.

— *Concernant les observations relatives à l'intelligence artificielle:*

L'IA est un modèle auto-apprenant exclusivement piloté par des ordinateurs.

Le programme SAS ne contient aucun module piloté par l'IA. Seules des techniques traditionnelles de *data mining* seront appliquées aux données du PCC, sans

te maken van artificiële intelligentie, in het kader van dossierselectie, selectie is niet hetzelfde als controle.

Er is dus altijd menselijke interventie. Er zijn nog geen testen uitgevoerd. Dit mag en kan op dit moment niet.

In eerste lezing is de minister reeds uitgebreid ingegaan op het SAS-programma. De software biedt talrijke geavanceerde statistische functie (reeksanalyses, distributieanalyses, simulaties, steekproeftrekkingen, correlatie- en netwerkanalyses, enz.). Deze functionaliteiten zijn wetenschappelijke statistische tools en vormen dus geen volledige automatische algoritmes die automatisch zorgen voor een controle.

— *Wat betreft de vragen naar kennisgevingsplicht:*

Er is geen kennisgeving aan belastingplichtigen bij de consultatie van het CAP door de fiscus, maar als de fiscus verlengde termijnen voor fraude gebruikt moet ze de aanwijzingen voor belastingontduiking uiteraard aan de belastingplichtige communiceren en dit op straffe van nietigheid (artikel 333, derde lid, van het WIB92). Dat is altijd het geval, en hier niet anders.

— *Er werd ook gevraagd naar de verhouding tussen de papieren en digitale aangiften in de personenbelasting*

Dit heeft niets met het voorliggende wetsontwerp te maken, een schriftelijke vraag is het gepaste instrument om cijfers en statistieken op te vragen. De minister tracht deze vragen stip en correct beantwoord.

— *Wat betreft GDPR controles:*

De FOD Financiën verwerkt persoonsgegevens in overeenstemming met de Algemene Verordening Gegevensbescherming. Zoals de minister reeds meermaals heeft vermeld, is er ook een functionaris voor de gegevensbescherming, de *data protection officer*. Bovendien moet elke fiscale ambtenaar natuurlijk de deontologische code en de richtlijnen bij het gebruik van informaticamiddelen respecteren.

Via diverse trainingen kunnen medewerkers van de FOD de benodigde vaardigheden ontwikkelen voor tal van zaken, ook voor GDPR, anonieme datamining etc.

recours à l'intelligence artificielle, dans le cadre de la sélection des dossiers. Sélectionner, ce n'est pas contrôler.

Il y a donc toujours une intervention humaine. Aucun test n'a encore été effectué. Les tests ne sont ni autorisés ni possibles pour le moment.

Lors de la première lecture, le ministre a déjà amplement évoqué le programme SAS. Ce logiciel offre de nombreuses fonctions statistiques avancées (analyses de séries, analyses de distribution, simulations, échantillonnages, analyses de corrélation et de réseau, etc.). Ces fonctionnalités sont des outils statistiques scientifiques et ne constituent donc pas des algorithmes entièrement automatiques qui donnent systématiquement lieu à un contrôle.

— *S'agissant des questions relatives à l'obligation de notification:*

Les contribuables ne reçoivent pas de notification lorsque le fisc consulte le PCC, mais si le fisc utilise des délais étendus au motif de présomption de fraude, il est bien entendu tenu de communiquer les indices d'évasion fiscale au contribuable, à peine de nullité (article 333, alinéa 3, du CIR92). C'est toujours le cas et il n'en va pas autrement en l'espèce.

— *Une question a également été posée concernant le rapport entre les déclarations papier et les déclarations en ligne dans le cadre de l'impôt des personnes physiques*

Ce sujet n'a rien à voir avec le projet de loi à l'examen. Une question écrite est l'instrument approprié pour demander des chiffres et des statistiques. Le ministre s'efforce de répondre à ces questions de manière précise et correcte.

— *En ce qui concerne les contrôles RGPD*

Le SPF Finances traite les données à caractère personnel conformément au Règlement général sur la protection des données. Comme le ministre l'a déjà mentionné à plusieurs reprises, il existe également un délégué à la protection des données, le *data protection officer*. En outre, il va de soi que chaque agent du fisc doit respecter le code déontologique et les directives lorsqu'il utilise des ressources informatiques.

Grâce à diverses formations, les collaborateurs du SPF peuvent développer les compétences nécessaires dans de nombreux domaines, et ce également en ce qui concerne le RGPD, le *data mining* anonyme, etc.

— *Over alle vragen over andere systemen in het buitenland:*

De minister wijst erop dat het hier aanpassingen aan het Belgische CAP betreft, niet een andere Europese vergelijkbare instantie. De minister zal zich dus niet uitspreken over alle buitenlandse voorbeelden die zijn gegeven, hoe boeiend deze ook mogen zijn.

— *Wat betreft de perceptie van de Belgen over het CAP:*

Hierover bestaan geen peilingen. Deze coalitie, die een meerderheid heeft in de Kamer van volksvertegenwoordigers, maakt van effectieve fraudebestrijding echter een prioriteit. De maatregel inzake het CAP kan daartoe bijdragen.

— *Wat betreft de vraag naar het aantal medewerkers, de verdeling van de VTE's en het budget van het CAP:*

Wat de betalingen aan de NBB betreft antwoordt de minister dat de NBB uiteraard het verbod op monetaire financiering moet naleven. Alle door de NBB gemaakte kosten moeten worden terugbetaald.

Vijf medewerkers van de NBB houden zich bezig met het beheer van het CAP, hetgeen 4,5 VTE's vertegenwoordigt.

Het leeuwendeel van de werkingskosten van de NBB heeft betrekking op de loonkosten van die 4,5 VTE's alsook op de operationele kosten die verband houden met de IT-infrastructuur die de werking van het CAP ondersteunt. De totale werkingskosten van het CAP bedragen ongeveer 2 miljoen euro per jaar.

Er is tot op heden nooit een datalek geweest met betrekking tot de gegevens van het CAP.

Om de bijzonder delicate persoonsgegevens van het CAP maximaal te vrijwaren van pogingen tot onwettige inzage heeft de NBB beslist deze gegevens niet in een publieke cloudomgeving maar in een "on-premise"-IT omgeving te herbergen en te verwerken. Om dezelfde veiligheidsredenen kan de NBB niet verder in te gaan over technische specificaties van haar IT-architectuur.

— *Is er overleg is geweest met Febelfin over de anonieme datamining en het CAP?*

De minister antwoordt dat Febelfin inderdaad aan de beleidscel haar opmerkingen op de betrokken bepalingen

— *En ce qui concerne toutes les questions relatives aux autres systèmes à l'étranger:*

Le ministre souligne que le projet à l'examen vise à modifier le PCC belge, et non une autre instance européenne comparable. C'est pourquoi le ministre ne se prononcera pas sur tous les exemples étrangers évoqués, aussi passionnants soient-ils.

— *En ce qui concerne la manière dont les Belges perçoivent le PCC:*

Il n'existe aucun sondage à ce sujet. La coalition actuelle, qui dispose d'une majorité à la Chambre des représentants, fait toutefois de la lutte efficace contre la fraude une priorité. La mesure relative au PCC pourra y contribuer.

— *En ce qui concerne la question relative au nombre de collaborateurs, à la répartition des ETP et au budget du PCC:*

En ce qui concerne les paiements à la BNB, le ministre répond que la BNB doit évidemment respecter l'interdiction d'un financement monétaire. Tous les frais engagés par la BNB doivent être remboursés.

Cinq collaborateurs de la BNB s'occupent de la gestion du PCC, ce qui représente 4,5 ETP.

La majorité des frais de fonctionnement de la BNB concerne les coûts salariaux de ces 4,5 ETP ainsi que les coûts opérationnels liés à l'infrastructure informatique qui soutient le fonctionnement du PCC. Les frais de fonctionnement totaux du PCC s'élèvent à environ 2 millions d'euros par an.

À ce jour, aucune fuite de données du PCC ne s'est encore produite.

Afin de protéger au maximum les données à caractère personnel particulièrement sensibles du PCC contre toute tentative d'accès illégal, la BNB a décidé de ne pas héberger ni traiter ces données dans un environnement *cloud* public, mais dans un environnement informatique "sur site". Pour les mêmes raisons de sécurité, la BNB ne peut fournir davantage de détails sur les spécifications techniques de son architecture informatique.

— *Une concertation a-t-elle eu lieu avec Febelfin concernant le data mining anonyme et le PCC?*

Le ministre répond que Febelfin a effectivement transmis ses observations sur les dispositions concernées à

heeft overgemaakt waarbij zij bijkomende vragen had over de manier waarop een rapportering moet gebeuren.

— *Wat betreft de vraag over realtime rapportering:*

De informatieplichtigen moeten de meeste info aan het CAP meedelen binnen vijf werkdagen, dus in die zin is er effectief geen realtime reporting van de gegevens door informatieplichtigen aan het CAP. De raadpleging van de gegevens opgenomen in het CAP door informatiegerechtigden (al dan niet via hun centraliserende organisaties) gebeurt wel in real time.

— *Wat betreft de vraag naar de plannen van de toekomst en efficiëntie en evaluatie:*

De minister antwoordt dat de plannen van de regering met betrekking tot het CAP terug te vinden zijn in het regeerakkoord, op pagina 46. Als er zaken efficiënter kunnen gebeuren dan zal de minister dat niet nalaten. Hetgeen voorligt in deze wetsartikelen moet in ieder geval de fraudebestrijding efficiënter maken.

Het CAP is belangrijk voor de fiscale fraudebestrijding, dat is niet nieuw. Het spreekt volgens de minister voor zich dat telkens moet bekeken worden of de huidige maatregelen efficiënt en effectief zijn. Dat is met andere maatregelen niet anders. Het Rekenhof speelt daarbij een belangrijke rol

Tot op heden zijn er geen externe evaluaties geweest, aangezien er evenmin klachten zijn geweest.

— *Wat betreft de vraag naar opleidingen:*

Ook hierop heeft de minister reeds antwoord gegeven in de eerste lezing. De FOD Financiën voorziet in tal van interne opleiding. Specifiek voor anonieme datamining heeft de minister in de eerste lezing reeds gezegd dat de noodzakelijke profielen reeds actief zijn bij de administratie. Er zijn er ongeveer twee à drie per algemene administratie.

Er zijn verschillende opleidingen binnen de FOD Financiën: SAS Enterprise Guide (*Querying and Reporting*), SAS Programming (*Essentials & Data Manipulation Techniques, Advanced Techniques and Efficiencies*), SAS Macro Language, SAS Visual Analytics (*Basics & advanced*), Basisopleiding ICT, Basisopleiding LEAN, Basisopleiding BPM, Projectmanagement, Privacy & Security (DAM-fiche).

la cellule stratégique. La fédération a notamment posé des questions complémentaires sur les modalités du rapportage.

— *En ce qui concerne la question relative au rapportage en temps réel:*

Les redevables d'information doivent communiquer la majorité des informations au PCC dans un délai de cinq jours ouvrables. Il n'y a dès lors pas de rapportage en temps réel. En revanche, la consultation des données enregistrées dans le PCC par les personnes habilitées à recevoir l'information (que ce soit via leurs organisations centralisatrices ou non) a bien lieu en temps réel.

— *Concernant les futurs projets, l'efficacité et l'évaluation:*

Le ministre répond que les projets du gouvernement concernant le PCC sont décrits à la page 48 de l'accord de gouvernement. Si certains ajustements peuvent accroître l'efficacité, le ministre ne manquera pas de les mettre en œuvre. En tout état de cause, les dispositions à l'examen visent à optimiser la lutte contre la fraude.

Le PCC joue un rôle important dans la lutte contre la fraude fiscale, et ce n'est pas nouveau. Selon le ministre, il va sans dire qu'il convient d'évaluer en permanence l'efficacité des mesures en vigueur. Il en va d'ailleurs de même pour toutes les mesures. La Cour des comptes a un rôle important à jouer à cet égard.

Compte tenu de l'absence de plainte, aucune évaluation externe n'a encore eu lieu jusqu'à présent.

— *En ce qui concerne la question relative aux formations:*

Le ministre a déjà répondu à cette question au cours de la première lecture. Le SPF Finances propose de nombreuses formations internes. Pour ce qui est de la question spécifique du *data mining* anonyme, le ministre a déjà indiqué en première lecture que l'administration dispose déjà des profils nécessaires. Chaque administration générale compte en effet deux à trois personnes qualifiées.

Le SPF Finances organise diverses formations: SAS Enterprise Guide (*Querying and Reporting*), SAS Programming (*Essentials & Data Manipulation Techniques, Advanced Techniques and Efficiencies*), SAS Macro Language, SAS Visual Analytics (*Basic & Advanced*), Formation de base ICT, Formation de base LEAN, Formation de base BPM, Gestion de projet, Privacy & Security (fiche DAM).

— *Wat betreft de vraag over real time queries:*

Zoals de minister reeds zei, is er een validatiestap tussen de melding en de opname in de database, net om voor meer zekerheid te zorgen dat de gegevens correct zijn.

— *Wat betreft de vraag over de integratie van het CAP en het UBO:*

De minister antwoordt dat dergelijke integratie momenteel niet is voorzien.

— *Wat betreft de vraag over privacy-preserving analytics en homomorphic encryption:*

De minister antwoordt dat dit een verzamelnaam is voor technieken om inzichten uit data te halen zonder de persoonsgegevens te onthullen. Ook daar heeft de minister het al enorm uitgebreid over gehad.

De persoonsgegevens zijn vandaag ook onherkenbaar gemaakt, gepseudonimiseerd. Dit is een ferme grendel op het gebruik van persoonsgegevens.

— *Wat betreft de schalen van de boetes:*

De minister bevestigt dat er niets verandert aan de betreffende bepalingen. Deze zijn onveranderd sinds 2018.

— *Wat betreft het verband met de AMLA (EU Authority for Anti-Money Laundering and Countering the Financing of Terrorism)*

Het doel van AMLA, dat deel uitmaakt van het AML-package, bestaat in het verzekeren van een correcte en consistente interpretatie van de regels inzake preventieve witwasbestrijding binnen Europa. Daarnaast houdt AMLA toezicht op bepaalde onderworpen entiteiten en moet de instelling de samenwerking tussen “*Financial Intelligence Units*”, zoals de CFI/CTIF in België, verstevigen. Dat staat los van het CAP. De FOD Financiën en de beleidscel van de minister zullen in dit najaar nog verdere uitvoering geven aan het AML-package.

— *Wat betreft de vraag over VDMML en e-miner:*

De minister verwijst naar zijn antwoord op schriftelijke vraag nr. 132: De programma's VDMML en e-miner van

— *En ce qui concerne la question relative aux requêtes (queries) en temps réel:*

Comme le ministre l'a indiqué précédemment, une validation doit avoir lieu entre la communication des informations et leur enregistrement dans la base de données, précisément pour accroître l'exactitude de ces données.

— *En ce qui concerne la question relative à l'intégration du PCC et du registre UBO:*

Le ministre répond que cette intégration n'est pas à l'ordre du jour.

— *En ce qui concerne la question relative aux techniques d'analyse respectueuses de la vie privée et au chiffrement homophonique:*

Le ministre répond qu'il s'agit d'un ensemble de techniques permettant de déduire des informations à partir de données sans révéler les données à caractère personnel. Il ajoute qu'il s'est déjà très longuement attardé sur ce point également.

Les données à caractère personnel sont déjà pseudonymisées aujourd'hui, si bien que les personnes concernées ne peuvent pas être identifiées. Il s'agit d'un verrou solide permettant d'empêcher l'utilisation des données à caractère personnel.

— *En ce qui concerne l'échelle des amendes:*

Le ministre confirme que les dispositions concernées, qui datent de 2018, restent inchangées.

— *En ce qui concerne le lien avec l'ALBC (Autorité européenne de lutte contre le blanchiment de capitaux et le financement du terrorisme)*

L'ALBC, instituée dans le cadre des mesures visant à lutter contre le blanchiment de capitaux (LBC), vise à assurer une interprétation correcte et cohérente des règles en matière de prévention du blanchiment en Europe. En outre, elle supervise certaines entités et vise à renforcer la coopération entre les “cellules de renseignement financier”, telles que la CTIF en Belgique. Il n'y a pas de lien entre l'ALBC et le PCC. Le SPF Finances et la cellule stratégique du ministre poursuivront cet automne la mise en œuvre du train de mesures LBC.

— *En ce qui concerne la question relative aux logiciels VDMML et Enterprise Miner:*

Le ministre renvoie à sa réponse à la question écrite n° 132: les programmes VDMML et Enterprise

SAS, worden door de FOD Financiën gebruikt. Maar dat zijn geen autonome AI-systemen. Ook hier wordt de verwerking gedocumenteerd in de DAM (*Data Access Management*)-fiche, opnieuw ontworpen om de risico's en conformiteit met betrekking tot de AVG en de veiligheid van de verwerking te kaderen.

— *Wat betreft de interactie en de wisselwerking tussen de CRS (Common Reporting Standards) en het CAP en de uitbreiding van CRS naar crypto en digitale platformen:*

Het CAP bevat inderdaad geen financiële data zoals bijvoorbeeld dividenden of interesten. Dat is bij het CRS wel het geval.

Sinds 2023 wordt al informatie uitgewisseld over de activiteiten van verkopers op digitale platformen. Die uitwisseling verschilt echter compleet van de uitwisseling in het kader van de CRS. De uitwisseling van informatie over cryptoactiva en e-money (DAC8) is momenteel in voorbereiding en zal binnenkort (in het voorjaar) in deze commissie besproken worden.

— *In hoeverre worden crypto-activa gebruikt voor criminele activiteiten en hoe performant werkt justitie daarop? Hoeveel verbeurdverklaringen zijn er geweest?*

De minister antwoordt dat deze materie niet behoort tot zijn bevoegdheidspakket.

— *Vertaalfout in de passage inzake de crypto-activa*

De minister bevestigt dat het Nederlandstalige woord “reglement” in artikel 95/5 inderdaad moet vervangen worden als “verordening”. Het gaat inderdaad om een vertaalfout. Deze fout werd reeds rechtgezet door de diensten van de Kamer.

— *De concrete inwerkingtreding*

De minister antwoordt dat de inwerkingtreding duidelijk bepaald is in artikel 95/8 (*nieuw*) van het wetsontwerp. Het artikel luidt als volgt: “De bepalingen van dit hoofdstuk treden in werking op 1 december 2026. De eerste mededeling door de informatieplichtigen van de saldi van de effectenrekeningen en van de crypto-activarekeningen zal op de saldi van deze rekeningen op datum 31 december 2025 en 30 juni 2026 slaan.”

Miner de la société SAS sont utilisés par le SPF Finances, mais ce ne sont pas des systèmes d'intelligence artificielle autonomes. Le traitement des données est également documenté dans une fiche DAM (*Data Access Management*), afin de limiter les risques et d'assurer la conformité avec le RGPD ainsi que la sécurité du traitement.

— *En ce qui concerne les interactions entre le CRS (Common Reporting Standard) et le PCC, et l'élargissement du CRS aux crypto-actifs et aux plateformes numériques:*

Contrairement au CRS, le PCC ne contient effectivement pas de données financières telles que les dividendes ou les intérêts.

Depuis 2023, des informations sont déjà échangées sur les activités des vendeurs sur les plateformes numériques. Cet échange ne correspond toutefois en rien aux échanges menés dans le cadre du CRS. La directive sur l'échange d'informations sur les crypto-actifs et les monnaies électroniques (DAC 8) est en préparation et sera bientôt examinée (au printemps) au sein de cette commission.

— *Dans quelle mesure les crypto-actifs sont-ils utilisés dans le cadre d'activités criminelles et quelle est l'efficacité de l'action de la justice en réponse à ces phénomènes? À combien s'élève le nombre de confiscations?*

Le ministre répond que cette matière ne relève pas de ses attributions.

— *Erreur de traduction dans le passage relatif aux crypto-actifs*

Le ministre confirme que dans le texte néerlandais de l'article 95/5, il convient de remplacer le mot “*reglement*” par le mot “*verordening*”. Il s'agit effectivement d'une erreur de traduction, qui a déjà été corrigée par les services de la Chambre.

— *Entrée en vigueur concrète*

Le ministre répond que la date d'entrée en vigueur est clairement précisée à l'article 95/8 (*nouveau*) du projet de loi, qui s'énonce comme suit: “Les dispositions du présent chapitre entrent en vigueur le 1^{er} décembre 2026. La première communication par les redevables d'information des soldes des comptes de titres et des comptes de crypto-actifs portera sur les soldes de ces comptes en date du 31 décembre 2025 et du 30 juin 2026.”

— *De andere maatregelen in het regeerakkoord inzake het CAP, met name bijvoorbeeld de gokrekeningen.*

De minister beaamt dat de gokrekeningen inderdaad niet werden opgenomen in de voorliggende wettekst. Dat zal in een volgende wet worden meegenomen.

— *De jaarlijkse taks op de effectenrekeningen*

Deze passage ligt in lijn met de aanbevelingen van het Rekenhof.

Wat betreft de vraag naar het onderscheid antwoordt de minister dat dit onderscheid wordt verantwoord door de noodzaak om het naleven van de voormelde specifieke antimisbruikbepaling inzake de jaarlijkse taks op effectenrekeningen te kunnen controleren.

— *Er werd gevraagd of “de ambtenaren alle gegevens gehouden door het CAP bekijken en samenvoegen, in het datawarehouse steken en er anonieme datamining op toepassen”.*

De minister antwoordt ontkennend. Er is een apart datamanagement systeem. In het amendement staat dit trouwens duidelijk: de ambtenaar moet de procedure van artikel 322 van het WIB92 volgen voor toegang tot de CAP-gegevens.

— *Wat betreft de opmerking dat het hier enkel gaat om een administratieve procedure:*

De minister bevestigt dat het hier om een administratieve procedure gaat. Dat is ook zeer logisch: er is nog geen vraag om inlichtingen gesteld, er is geen bericht van wijziging en zeker geen aanslagbiljet.

Er wordt op geen enkel moment afbreuk gedaan aan de rechten van de belastingplichtige. De tegensprekelijke procedure blijft van toepassing.

— *Wat betreft de vraag inzake Art 4.4 van de AVG:*

Een commissielid merkte het volgend op: “Het SAS bevat geen automatische algoritmes, hoe kunt u dat dan rijmen met het feit dat u zegt dat u zult gaan profileren, want dat is elke vorm van automatische verwerking van persoonsgegevens?”

— *Les autres mesures relatives au PCC prévues dans l'accord de gouvernement, notamment les comptes de paris en ligne*

Le ministre reconnaît que les comptes de paris en ligne ne sont pas visés par le projet de loi à l'examen. Ils devront dès lors être intégrés dans un projet de loi ultérieur.

— *La taxe annuelle sur les comptes-titres*

Ce passage donne suite aux recommandations de la Cour des comptes.

En réponse à la question relative à la distinction opérée, le ministre indique que celle-ci se justifie par la nécessité de contrôler le respect de la disposition anti-abus spécifique précitée dans le cadre de la taxe annuelle sur les comptes-titres.

— *Il a été demandé si les fonctionnaires examineraient et fusionneraient l'ensemble des données enregistrées dans le PCC avant de les intégrer dans le data warehouse et de procéder à des opérations de data mining anonyme.*

Le ministre répond par la négative. Un système de gestion des données distinct est prévu. C'est d'ailleurs clairement précisé dans l'amendement: les fonctionnaires concernés devront suivre la procédure d'accès au PCC visée à l'article 322 du CIR 92.

— *En ce qui concerne l'observation selon laquelle la procédure visée sera purement administrative:*

Le ministre confirme que la procédure visée sera purement administrative, ce qui est somme toute parfaitement logique: il n'y aura pas encore eu de demande de renseignement, ni d'avis de rectification et certainement pas d'avertissement-extrait de rôle.

Les dispositions en projet ne portent nullement atteinte aux droits des contribuables. La procédure contradictoire restera applicable.

— *En ce qui concerne la question relative à l'article 4.4 du RGPD:*

Un membre de la commission a formulé l'observation suivante: “Le SAS ne contient aucun algorithme automatique. Comment pouvez-vous alors concilier ce fait avec vos propos selon lesquels vous recourrez au profilage, qui est défini comme toute forme de traitement automatisé de données à caractère personnel?”

De minister antwoordt dat in de context van fiscale fraudedetectie deze datamining analyses mogelijk maakt om controles te richten op risicogebieden, waarbij het gebruik van beperkte middelen wordt geoptimaliseerd.

Correlaties die voortkomen uit bestandsvergelijkingen, statistieken of algoritmen zijn geen juridisch bewijs of bewijs van causaliteit. Ze moeten worden beschouwd als indicatoren of waarschuwingssignalen, niet als objectieve waarheden.

Analyses helpen, maar veroordelen niet. Ze zijn een instrument voor efficiëntie, geen juridische basis. Deze analyses worden gebruikt om controles te richten op risicogebieden, om middelen te optimaliseren, in plaats van willekeurige controles uit te voeren.

Als er problemen kunnen ontstaan in de analyses, moet de output van de datamining-analyses kritisch worden geanalyseerd op fouten (valse positieven of andere kwaliteitsproblemen) en moet het model indien nodig worden aangepast of gecorrigeerd. De werkprocessen bij de FOD Financiën maken het mogelijk om dergelijke fouten onafhankelijk te detecteren en te rapporteren en indien nodig te corrigeren. De projecten zijn iteratief en het selecteren van pilotbestanden maakt het mogelijk om de analyses van de dataminers te testen.

Elke beslissing moet worden voorafgegaan door menselijke tussenkomst en een geïndividualiseerd fiscaal onderzoek, met waarborgen om de rechten van belastingplichtigen onder de AVG en de wet van 3 augustus 2012 te beschermen, maar ook in overeenstemming met de wettelijk georganiseerde fiscale procedures en de wetten en principes van goed bestuur die van toepassing zijn op de FOD Financiën.

— *Mag de administratie alle informatie uit het CAP halen zonder enige reden?*

De minister benadrukt nogmaals dat de toegang tot het CAP altijd gebeurt binnen een strikt procedureel kader. Het antwoord is dus “neen”.

— *Moet een ambtenaar van de belastingen informatie die hij uit het CAP haalt delen met zijn collega's van de FOD?*

In het kader van anonieme datamining worden de gegevens gepseudonimiseerd verwerkt om risicoprofielen

Le ministre répond que, dans le contexte de la détection de la fraude fiscale, cette exploration de données permettra de procéder à des analyses visant à mener des contrôles dans des domaines à risques, ce qui permettra d'optimiser l'utilisation de moyens limités.

Les corrélations issues de comparaisons de fichiers, de statistiques ou d'algorithmes ne constituent ni des preuves juridiques ni des preuves de causalité. Elles doivent être considérées comme des indicateurs ou des signaux d'avertissement, et pas comme des vérités objectives.

Les analyses aident, mais ne permettent pas de condamner. Elles constituent un outil pour renforcer l'efficacité, mais pas une base juridique. Ces analyses seront utilisées pour mener des contrôles dans des domaines à risques, pour optimiser les moyens, au lieu d'effectuer des contrôles aléatoires.

Si des problèmes peuvent survenir dans les analyses, le résultat des analyses de l'exploration de données devra être analysé de manière critique en vue d'identifier les erreurs (faux positifs ou autres problèmes de qualité) et le modèle devra être modifié ou rectifié au besoin. Les processus de travail du SPF Finances permettent de détecter et de notifier en toute indépendance des erreurs de cette nature, et de les corriger si nécessaire. Les projets seront itératifs et la sélection de fichiers pilotes permettra de tester les analyses des explorateurs de données.

Toute décision devra être précédée d'une intervention humaine et d'une enquête fiscale individuelle, en garantissant la protection des droits conférés aux contribuables par le RGPD et par la loi du 3 août 2012, mais aussi en respectant les procédures fiscales prévues par la législation, ainsi que les lois et principes de bonne gestion applicables au SPF Finances.

— *L'administration pourra-t-elle utiliser toutes les informations contenues dans le PCC sans fournir la moindre justification?*

Le ministre souligne une nouvelle fois que l'accès au PCC sera toujours subordonné au respect d'une procédure stricte. Il répond donc à cette question par la négative.

— *Un fonctionnaire de l'administration fiscale doit-il partager avec ses collègues du SPF des informations qu'il obtient du PCC?*

Dans le cadre de l'exploration anonyme de données, les données seront traitées de manière pseudonymisée

te bepalen door gekwalificeerde dataminers. In dit stadium hebben deze gegevens dus geen enkel nut voor andere ambtenaren van de FOD Financiën, zelfs als zij er toegang toe zouden hebben.

Alleen in geval van aanwijzingen van fraude worden de gegevens in gedepseudonimiseerde vorm uitsluitend overgemaakt aan de ambtenaren die bevoegd zijn om de geselecteerde dossiers te controleren.

— *Er werd gesteld dat dit een “blanco-volmacht” is*

Gegevens blijven gepseudonimiseerd tijdens het dataminingproces en worden alleen gedepseudonimiseerd voor die specifieke dossiers waarin concrete risico's op inbreuken verschijnen.

— *Wat betreft de opmerkingen inzake GDPR*

De Europese regels primeren hiërarchisch op het Belgische recht. De rechten van de burger blijven volledig gewaarborgd. De gegevens zijn gepseudonimiseerd en kunnen slechts worden gedepseudonimiseerd bij concrete fraude-indicaties – precies zoals Europa het voorschrijft.

Alle GDPR-beginselen zijn, en blijven, van toepassing. Dit alles is van toepassing op de NBB, maar ook op diegenen die toegang hebben tot de gegevens, zoals de FOD Financiën. Ook dit is niets nieuws, hier verandert niets.

— *Wat betreft de termijnen, hoe lang worden de zaken bijgehouden?*

Er is een maximale bewaartermijn die één jaar na de verjaring van alle vorderingen die tot de bevoegdheid van de FOD behoren. Bovendien mag deze bewaartermijn de definitieve beëindiging van de administratieve en rechterlijke procedures en rechtsmiddelen en de integrale betaling van alle hiermee verbonden bedragen niet overschrijden. De FOD Financiën zal deze dus niet langer dan strikt noodzakelijk bewaren.

— *Er waren verschillende vragen over de pseudonimisering en de sleutels*

Het IT-security team binnen de FOD Financiën is verantwoordelijk om alle regels inzake toegang en cryptage vast te leggen.

pour que des explorateurs de données qualifiés définissent des profils de risque. À ce stade, ces données ne présenteraient donc aucune utilité pour d'autres fonctionnaires du SPF Finances, même s'ils y avaient accès.

Ce n'est qu'en cas d'indications de fraude que les données seront transmises, sous forme dépseudonymisées, exclusivement aux fonctionnaires habilités à contrôler les dossiers sélectionnés.

— *D'aucuns ont indiqué qu'il s'agissait d'un “blanc-seing”*

Les données resteront pseudonymisées pendant le processus d'exploration des données, et elles ne seront dépseudonymisées que dans les dossiers spécifiques présentant des risques concrets d'infractions.

— *En ce qui concerne les observations relatives au RGPD*

Dans la hiérarchie des normes, les règles européennes l'emportent sur le droit belge. Les droits des citoyens demeureront pleinement garantis. Les données seront pseudonymisées et ne pourront être dépseudonymisées qu'en cas d'indications concrètes de fraude, ce qui est exactement ce que prévoit la législation européenne.

Tous les principes du RGPD seront et resteront d'application. Toutes ces règles s'appliquent à la BNB, mais aussi aux institutions qui ont accès aux données, comme le SPF Finances. Ce n'est pas non plus nouveau, et rien ne changera à cet égard.

— *En ce qui concerne les délais, combien de temps les données seront-elles conservées?*

On prévoit un délai de conservation ne pouvant excéder un an après la prescription de toutes les actions qui relèvent de la compétence du SPF. En outre, ce délai de conservation ne pourra pas se prolonger au-delà de l'extinction des procédures et recours administratifs et judiciaires, ainsi que du paiement intégral de tous les montants y afférents. Le SPF Finances ne conservera donc pas ces données plus longtemps que ce qui sera strictement nécessaire.

— *Plusieurs questions ont été posées au sujet de la pseudonymisation et des clés*

L'équipe chargée de la sécurité informatique au sein du SPF Finances est responsable de définir toutes les règles en matière d'accès et de cryptage.

Sleutels worden in een zogenaamde “vault-applicatie” bewaard. Bij elke processing wordt een andere sleutel gebruikt.

Deze ambtenaren hebben geen verband met de fiscale diensten. Er is steeds een menselijke tussenkomst.

— *Is er sprake van een onafhankelijke sleutelbewaring?*

In casu is dit de door de voorzitter van het directiecomité van de FOD Financiën aangeduide vertrouwde derde partij (onafhankelijk en zonder hiërarchische band met de fiscus) na overleg met de DPO en is specifiek verantwoordelijk voor de coördinatie en controle van alle verwerkingen die door de FOD Financiën worden uitgevoerd met betrekking tot de CAP-gegevens. Deze vertrouwde derde partij zal als enige de technische sleutels bezitten en bewaren die kruisingen mogelijk maken zonder directe identificatie.

— *Wat betreft de opmerkingen over de risicofactoren, en het feit dat er geen onderscheid tussen klein of groot risico wordt gemaakt of geen minimumbedrag wordt ingevoerd*

De minister herhaalt nogmaals dat het een dossierselectie betreft. Selectie is niet gelijk aan controle

Om het heel eenvoudig te schetsen maakt de minister een vergelijking met een alcoholcontrole door de politie: De zwalpende auto zal worden gecontroleerd, maar daarmee is er nog geen enkel onderzoek of dergelijke gebeurd. Het blazen in de combi, moet dan nog plaatsvinden en enkel dat zal bepalen of men een boete krijgt, niet per se het zwalpend rijden. Het kan zijn dat die persoon zwalpend reed om iets te ontwijken of omwille van een technisch defect, dan is dat uiteraard geen probleem.

Iemand die even 121 km per uur rijdt op de autostrade, daar gaat de politie zich niet actief mee bezighouden. Al moet de minister voor de volledigheid wel toevoegen dat enkele jaren geleden wel de tolerantie marge werd afgeschaft.

De minister heeft reeds geschetst wat er in de DAM-fiches wordt opgenomen. Opnieuw, dit is de interne strategie van de FOD Financiën, maar het spreekt voor zich dat dit niet voor een eenvoudige storting van wat cash op de rekening dient noch voor alle andere voorbeelden die hier zijn gemaakt.

Les clés sont conservées dans une “application coffre-fort”. Une clé différente est utilisée pour chaque traitement.

Ces fonctionnaires n’ont aucun lien avec les services fiscaux. Une intervention humaine est toujours prévue.

— *La conservation des clés se fera-t-elle en toute indépendance?*

En l’espèce, le tiers de confiance (indépendant et libre de tout lien hiérarchique avec l’administration fiscale) désigné par le président du comité de direction du SPF Finances après concertation avec le DPO sera spécifiquement responsable de la coordination et du contrôle de tous les traitements des données extraites du PCC effectués par le SPF Finances. Ce tiers de confiance sera le seul à posséder et à conserver les clés techniques permettant de réaliser des croisements de données sans identification directe.

— *S’agissant des observations sur les facteurs de risque, et le fait qu’aucune distinction ne sera opérée entre les risques minimales et les risques majeurs, ou qu’aucun montant minimum ne sera fixé*

Le ministre répète une nouvelle fois que l’exploration des données servira à sélectionner des dossiers. Or, sélection n’est pas synonyme de contrôle.

Pour l’expliquer de manière très simple, le ministre fait une comparaison avec les contrôles anti-alcoolémie de la police: un véhicule qui zigzague sera contrôlé, même en l’absence d’enquête ou d’autre mesure. Il faudra alors encore réaliser un contrôle par éthylotest dans le combi, et lui seul permettra de déterminer si une amende sera infligée, et pas forcément le fait que le conducteur zigzagait. Il se pouvait en effet que celui-ci zigzagait pour éviter un obstacle ou à cause d’un problème technique, auquel cas aucun problème ne se pose évidemment.

La police ne va pas s’occuper en priorité des conducteurs qui roulent à 121 km/h sur l’autoroute, même si le ministre doit ajouter, par souci d’exhaustivité, que la marge de tolérance en la matière a été supprimée il y a quelques années.

Le ministre a déjà décrit le contenu des fiches DAM. Il réitère qu’il s’agit de la stratégie interne du SPF Finances, mais il est évident que cela ne vaut pas pour le simple versement d’un faible montant en liquide sur un compte, ni pour tous les autres exemples qui sont donnés en l’occurrence.

Een lid stelde de vraag waarom er geen minimum-bedrag wordt ingevoerd. De minister antwoordt dat een minimumdrempel niet werd voorzien bij de wet van 20 december 2020 door de vorige regering. De regering oordeelde toen “dat dit de financiële instellingen zou opzadelen met ernstige technische moeilijkheden”. Op de toenmalige kritiek van de Gegevensbeschermingsautoriteit werd er door de vorige regering op gewezen dat “De informatie waarover het CAP beschikt, ook kan gebruikt worden door het gerecht, o.a. in het kader van onderzoeken naar witwassen van geld, financiering van terrorisme en zware criminaliteit. In het verleden is vastgesteld dat criminele organisaties dikwijls een groot aantal transacties uitvoeren met een relatief klein bedrag. Kortom, een veelheid van rekeningen met een klein saldo kan juist een belangrijke parameter zijn bij de beoordeling door de gerechtelijke instanties om een onderzoek op te starten”.

Het niet-invoeren van een minimumdrempel houdt ook in dat de saldi van de rekeningen van alle minderjarigen worden meegedeeld aan het CAP. Ook dat was reeds het geval tijdens de vorige regering. Er dus niets nieuws aan toegevoegd.

— *Kan via het CAP elke inbreuk op enige fiscale wetgeving worden gecontroleerd? (Taksen, inkomstenbelasting, btw, ...?)*

Dit wordt per wetboek of wet geregeld. Artikel 322 van het WIB92 bevat dit voor de inkomstenbelastingen. Het artikel 95/1 doet dit net voor het Wetboek Diverse Rechten en Taksen en dan specifiek voor de jaarlijkse taks op de effecentrekeningen.

— *Er werd verwezen naar arrest C-817/19 over het PNR-systeem*

De feiten in het arrest C-817/19 van 21 juni 2022 van het Europees Hof van Justitie en het arrest nr. 131/2023 van 12 oktober 2023 van het Grondwettelijk Hof zijn geenszins te vergelijken met wat in het ontworpen artikel voorligt.

De feiten in dit arrest zijn anders, het gaat niet om dezelfde gegevens of dezelfde risico's, aangezien het gaat om de strijd tegen terrorisme. Wel kan men de proportionaliteit ten opzichte van het nagestreefde doel evalueren wanneer de verwerking van persoonsgegevens wordt geautomatiseerd.

In de context van het huidige wetsontwerp en gezien de garanties die daarin zijn voorzien om te voldoen aan de eisen van de AVG, wordt hieraan volgens de minister voldaan.

Un membre a demandé pourquoi aucun montant minimum n'était prévu. Le ministre répond qu'un seuil minimum n'avait pas été prévu par le gouvernement précédent dans la loi du 20 décembre 2020. À l'époque, le gouvernement avait en effet estimé que cela “entraînerait de sévères complications techniques” pour les établissements financiers. En réponse à la critique formulée alors par l'Autorité de protection des données, le précédent gouvernement avait indiqué que “les informations dont disposent le PCC peuvent aussi être utilisées par la Justice, notamment dans le cadre d'enquêtes sur des faits de blanchiment d'argent, de financement du terrorisme et de grande criminalité. Par le passé, il a été constaté que les organisations criminelles effectuaient souvent un grand nombre de transactions de montants relativement faibles. En résumé, une multitude de comptes à petit solde peut en fait être un paramètre important dans l'évaluation réalisée par les autorités judiciaires pour déterminer l'opportunité d'ouvrir ou non une enquête.”

La non-instauratation d'un seuil minimum implique aussi que les soldes des comptes de tous les mineurs d'âge soient aussi communiqués au PCC. Tel était aussi déjà le cas sous le gouvernement précédent. Il n'y aura donc aucune nouveauté en la matière.

— *Le PCC permet-il de contrôler toute infraction à n'importe quelle législation fiscale (taxes, impôts sur les revenus, TVA, etc.)?*

Cette possibilité est réglée par code ou par loi. L'article 322 du CIR92 la prévoit pour les impôts sur les revenus. L'article 95/1 du projet de loi introduit cette possibilité dans le Code des droits et taxes divers, spécifiquement pour la taxe annuelle sur les comptes-titres.

— *Renvoi à l'arrêt C-817/19 sur le système PNR.*

Les faits évoqués dans l'arrêt C-817/19 du 21 juin 2022 de la Cour européenne de justice et dans l'arrêt n° 131/2023 du 12 octobre 2023 de la Cour constitutionnelle ne sont nullement comparables au contenu de l'article en projet.

Les faits cités dans cet arrêt sont d'une autre nature. Ils ne concernent pas les mêmes données ni les mêmes risques, puisqu'ils s'inscrivent dans la lutte contre le terrorisme. On peut toutefois évaluer la proportionnalité par rapport à la finalité, lorsque le traitement de données à caractère personnel est automatisé.

Dans le cadre du projet de loi à l'examen et des garanties qui y sont prévues pour répondre aux exigences du RGPD, le ministre estime que le critère de la proportionnalité est respecté.

— Een lid merkte nogmaals op dat er een automatische controle is

Er vindt geen automatische besluitvorming plaats. De anonieme datamining heeft enkel tot doel om efficiënter en gerichtere dossierselectie te bewerkstelligen.

— Wat met valse positieven?

De minister antwoordt dat er net daarom een menselijke tussenkomst is. De minister verwijst nogmaals naar zijn reeds uitgebreide antwoord in de eerste lezing.

De “machine” neemt geen beslissingen, maar biedt ondersteuning aan de persoon die de beslissing zal nemen. Controleurs verifiëren de afwijkingen en de dossiers met het hoogste risico voordat ze worden voorgesteld voor controle, en de uitvoering van de controle is eveneens aan goedkeuring onderworpen van een hogere ambtenaar.

Die menselijke tussenkomst wordt bovendien gereguleerd door strikte regels: een gedefinieerd werkproces met scheiding van functies, beperkingen op basis van de gevoeligheid van de gegevens en het doel, logging van toegang en audits.

Zo zijn er maar enkele bevoegde personen die de “sleutel” hebben om de gegevens te depseudonimiseren, wat op zijn beurt opnieuw bijdraagt aan een betere bescherming van het privéleven.

7. Besluit

De minister besluit dat de datamining in het CAP een instrument is in de strijd tegen fiscale fraude en georganiseerde criminaliteit.

De maatregel inzake het CAP voorstellen alsof in de toekomst iedereen een potentiële fraudeur is, alsof de fiscus in uw bankapp zit, is de waarheid geweld aandoen.

C. Replieken van de leden

Mevrouw Charlotte Verkeyn (N-VA) dankt de minister voor de uitgebreide antwoorden en voor de geboden geruststellingen.

Zij formuleert vervolgens twee bijkomende opmerkingen die, naar haar oordeel, nuttig zijn om in het verslag op te nemen.

— Un membre a de nouveau relevé le caractère automatique du contrôle

Aucune décision n'est prise automatiquement. Le *data mining* anonyme a uniquement pour but de rendre la sélection des dossiers plus efficace et plus ciblée.

— Qu'en est-il des faux positifs?

Le ministre répond que c'est précisément pour cette raison qu'il y a une intervention humaine. Il se réfère de nouveau à la réponse détaillée qu'il a déjà fournie lors de la première lecture.

La “machine” ne prend pas de décision, elle assiste la personne qui prendra la décision. Les contrôleurs vérifient les anomalies et les dossiers présentant le risque le plus élevé avant que ceux-ci soient proposés en vue d'un contrôle. La réalisation du contrôle est en outre soumise à l'approbation d'un fonctionnaire supérieur.

Par ailleurs, cette intervention humaine est strictement régulée: définition d'un processus de travail avec une séparation des fonctions, restrictions liées à la sensibilité des données et à la finalité, enregistrement des accès dans un journal et réalisation d'audits.

Ainsi, seules quelques personnes habilitées disposent de la “clé” permettant de depseudonymiser les données, ce qui contribue également à renforcer la protection de la vie privée.

7. Conclusion

Le ministre conclut en indiquant que le *data mining* pratiqué sur le PCC représente un instrument de plus dans la lutte contre la fraude fiscale et la criminalité organisée.

Faire croire qu'avec la mesure relative au PCC, chaque contribuable sera désormais considéré comme un fraudeur potentiel et que l'administration fiscale fouinera dans l'application bancaire des clients, c'est trahir la vérité.

C. Répliques des membres

Mme Charlotte Verkeyn (N-VA) remercie le ministre pour ses réponses détaillées et ses mises au point rassurantes.

Elle formule ensuite deux remarques supplémentaires qui, selon elle, devraient figurer dans le rapport.

Zij verwijst naar de bespreking van vorige week, waarin de situaties in Cyprus en Malta niet aan bod kwamen. Polen werd toen evenmin besproken, maar spreekster wenst vandaag toch stil te staan bij de Poolse situatie.

Meer in het bijzonder gaat ze in op het Europees verbod inzake staatssteun, aangezien meerdere leden, onder anderen collega's Matheï, Vereeck, D'Amico, Vanbesien en Van Quickenborne, tijdens de eerste lezing vragen formuleerden over mogelijke problemen op het vlak van staatssteun.

Mevrouw Verkeyn wijst er op dat er intussen een zeer recent arrest van het Hof van Justitie beschikbaar is: het arrest van 25 april 2025 in de zaak *Prezydent Miasta Mielca* (burgemeester van de stad Mielec) (C-453/23). Dit arrest stelt vast dat een algemene en abstracte vrijstelling geacht wordt inherent te zijn aan het normale belastingstelsel, zodat zo'n vrijstelling over het algemeen geen selectief voordeel kan verlenen en dus normaliter geen staatssteun uitmaakt. Zij merkt op dat de derde kamer van de Raad van State in zijn advies van 22 mei 2025, dit arrest, gezien de datum, nog niet kon meenemen, hoewel het uitgesproken is door de Grote Kamer van het Hof van Justitie en daarom aanzienlijk weegt in de rechtsontwikkeling. Volgens mevrouw Verkeyn weerlegt dit arrest een groot deel van de kritiek die tijdens de eerste lezing werd geuit.

Ter staving van haar stelling verwijst ze ook naar een recente bijdrage in het vaktijdschrift *Fiscale Actualiteit* van Joris Lutz en Melanie Massin, waarin dezelfde conclusie wordt getrokken: de elementen in het wetsontwerp die aanleiding gaven tot bezorgdheden, blijken in het licht van het arrest niet strijdig met de staatssteunregels. Zo vormt bijvoorbeeld de expatregeling een onderdeel van het referentiestelsel en dus geen afwijking.

Ook met betrekking tot het debat over het flexi-jobplafond acht mevrouw Verkeyn het arrest relevant. Zij stelt vast dat er, toen er nog geen fiscaal plafond bestond, geen vragen werden gesteld over mogelijke staatssteun, maar dat die vragen pas opdoken nadat de vorige regering een niet-geïndexeerd plafond invoerde. Volgens haar past de redenering uit het Poolse arrest perfect: flexi-jobs vormen een algemene maatregel waarvan het fiscale voordeel uitsluitend toekomt aan natuurlijke personen die geen onderneming zijn en ze leveren geen enkele kostenbesparing op voor werkgevers. Dit strookt, aldus mevrouw Verkeyn, volledig met de logica van het arrest.

L'intervenante renvoie à la discussion de la semaine dernière, lors de laquelle les situations à Chypre et à Malte n'ont pas été évoquées. L'exemple de la Pologne n'a pas non plus été cité, mais la membre souhaite se pencher aujourd'hui sur la situation dans ce pays.

La députée aborde en particulier l'interdiction européenne des aides d'État, puisque plusieurs membres, dont les collègues Matheï, Vereeck, D'Amico, Vanbesien et Van Quickenborne, ont posé des questions, lors de la première lecture, concernant d'éventuels problèmes en matière d'aides d'État.

Mme Verkeyn fait référence à un arrêt très récent de la Cour européenne de justice, l'arrêt C-453/23 du 25 avril 2025 dans l'affaire *Prezydent Miasta Mielca* (bourgmestre de la ville de Mielec). Dans cet arrêt, la Cour indique qu'une exonération générale et abstraite est présumée être inhérente au régime fiscal normal, de sorte que pareille exonération ne saurait, en règle générale, conférer un avantage sélectif et échappe dès lors normalement à la qualification d'"aide d'État". L'intervenante relève que la troisième chambre du Conseil d'État ne pouvait pas encore prendre en compte cet arrêt, en raison du délai, dans son avis du 22 mai 2025, bien que cet arrêt ait été rendu par la Grande Chambre de la Cour de justice et qu'il ait dès lors un poids considérable dans l'évolution du droit. Selon Mme Verkeyn, l'arrêt en question réfute une grande partie des critiques émises lors de la première lecture.

Pour étayer sa position, elle renvoie encore à un article récent de Joris Lutz et Melanie Massin, publié dans la revue spécialisée *Fiscale Actualiteit*, qui arrive à la même conclusion: il s'avère, à la lumière de l'arrêt, que les éléments du projet de loi qui suscitaient des inquiétudes ne sont pas contraires aux règles en matière d'aides d'État. Par exemple, le régime applicable aux expatriés fait partie du régime de référence et ne constitue donc pas une dérogation.

Mme Verkeyn estime aussi que l'arrêt est pertinent dans le débat sur le plafond relatif aux flexi-jobs. Elle observe qu'aucune question ne se posait sur une éventuelle aide d'État à l'époque où il n'existait pas encore de plafond fiscal, mais que ces questions n'ont surgi qu'après l'instauration par le gouvernement précédent d'un plafond non indexé. Selon elle, le raisonnement suivi dans l'arrêt polonais est parfaitement applicable en l'occurrence: les flexi-jobs constituent une mesure générale, dont l'avantage fiscal revient exclusivement aux personnes physiques qui ne sont pas des entreprises, et ne procurent aucune réduction de coûts aux employeurs. Selon Mme Verkeyn, ce raisonnement correspond totalement à la logique de l'arrêt.

Dit arrest geldt ook voor het belastingkrediet voor eigen middelen voor alle zelfstandigen.

In een tweede deel van haar tussenkomst wenst mevrouw Verkeyn een rechtzetting te formuleren naar aanleiding van de opmerkingen van collega Vanbesien tijdens de bespreking in eerste lezing. In het verslag zou staan dat zij zou hebben verklaard dat het leefloon niet meetelt bij de berekening van de personen ten laste. Zij verwijst naar de laatste zin van het verslag, waarin precies wordt vastgesteld dat vanaf de eerste eurocent aan leefloon een persoon voortaan niet meer als ten laste wordt beschouwd. Zij illustreert met een vergelijking: een zoon die één euro verdient die als beroepskosten worden aangemerkt in de zaak van zijn vader, wordt niet langer als ten laste beschouwd. Activering blijft volgens haar de beste manier om mensen uit armoede te helpen, en daarom is het logisch dat iemand die ook maar één euro leefloon ontvangt, niet langer als fiscaal ten laste kan worden aangemerkt van hetzelfde huishouden, en dit tot in de tweede graad.

De heer Lode Vereeck (VB) dankt eveneens de minister voor de beantwoording van de vragen. Hij opent zijn tussenkomst met een bespreking van de flexijobs.

Wat de fiscaliteit betreft, merkt hij op – en verwijst daarbij naar de eerdere bevestiging door mevrouw Verkeyn – dat er volgens de regering geen sprake zou zijn van staatssteun, aangezien het voordeel rechtstreeks wordt toegekend aan natuurlijke personen. Toch wijst hij erop dat ondernemingen die voor flexi-jobwerknemers geen bedrijfsvoorheffing moeten inhouden, onmiskenbaar een economisch voordeel genieten. Dat punt mag volgens hem niet uit het oog worden verloren.

Vervolgens herhaalt de heer Vereeck zijn bezorgdheid over een mogelijke ongelijke behandeling tussen verschillende categorieën voltijdswerkenden. Hij verwijst naar het onderscheid tussen iemand die voltijds (vijf vijfde) werkt in één enkele functie, en iemand die vier vijfde werkt en daarnaast een vijfde flexi-job verricht. In het eerste geval bedraagt de belastingvrije som 10.570 euro, terwijl dit in het tweede geval oploopt tot 22.570 euro. Dit verschil beschouwt hij als een mogelijke vorm van fiscale discriminatie.

De spreker heeft de bestaande arresten van het Grondwettelijk Hof geraadpleegd, waarin werd geoordeeld dat flexi-jobs in verschillende opzichten niet discrimineren. Hij verwijst onder meer naar de arresten nrs. 107/2017, 25/2008 en 25/2006. Die arresten behandelen echter andere situaties, zoals het onderscheid tussen gepensioneerde en niet-gepensioneerde flexiwerkers, tussen flexiwerkers in verbonden en niet-verbonden

Cet arrêt s'applique aussi au crédit d'impôt pour fonds propres pour tous les indépendants.

Dans une deuxième partie de son intervention, Mme Verkeyn souhaite apporter une rectification aux propos tenus par M. Vanbesien lors de la discussion en première lecture. Le rapport indiquerait qu'elle aurait déclaré que le revenu d'intégration ne compte pas dans le calcul des personnes à charge. Elle renvoie à la dernière phrase du rapport, qui précise justement que dès le premier centime d'euro de revenu d'intégration, une personne n'est plus considérée comme à charge. Elle cite un exemple à titre de comparaison: un fils qui gagne un seul euro qualifié de frais professionnels dans l'entreprise de son père n'est plus considéré comme fiscalement à charge. Selon elle, l'activation demeure la meilleure manière de sortir les personnes de la pauvreté. Par conséquent, il est logique qu'une personne percevant ne fût-ce qu'un euro de revenu d'intégration ne puisse plus être considérée comme fiscalement à charge du même ménage, et ce, jusqu'au deuxième degré.

M. Lode Vereeck (VB) remercie également le ministre pour ses réponses. Il entame son intervention en évoquant la question des flexi-jobs.

En ce qui concerne la fiscalité, il note — tout en se référant à la confirmation précédente de Mme Verkeyn — que, selon le gouvernement, il ne s'agit pas d'aides d'État, car l'avantage est directement accordé aux personnes physiques. L'intervenant attire néanmoins l'attention sur le fait que les entreprises qui ne doivent retenir aucun précompte professionnel pour les flexi-jobbeurs bénéficient indéniablement d'un avantage économique. Selon l'intervenant, il ne faut pas négliger ce point.

Ensuite, M. Vereeck réitère son inquiétude quant à une éventuelle inégalité de traitement entre différentes catégories de travailleurs à temps plein. Il mentionne la distinction entre une personne travaillant à temps plein (à raison de cinq cinquièmes) dans une seule fonction et une personne travaillant à quatre cinquièmes et effectuant en plus un flexi-job à raison d'un cinquième. Dans le premier cas, la quotité exemptée s'élève à 10.570 euros, tandis que, dans le second cas, elle atteint 22.570 euros. Il considère cette différence comme une forme potentielle de discrimination fiscale.

L'intervenant a consulté les arrêts de la Cour constitutionnelle selon lesquels les flexi-jobs ne sont pas discriminatoires à plusieurs égards. Il renvoie notamment aux arrêts n° 107/2017, 25/2008 et 25/2006, mais ajoute que ces derniers portent sur d'autres questions, par exemple sur la distinction entre les flexi-jobbeurs retraités et non retraités, entre les flexi-jobbeurs employés dans des entreprises liées et non liées, ou entre les

ondernemingen, of tussen horecaondernemingen met en zonder witte kassa. In al deze gevallen werd geen discriminatie vastgesteld, en hetzelfde geldt voor de beoordeling van overgangsregelingen voor werknemers die overstappen naar een viervijfde tewerkstelling.

De heer Vereeck benadrukt echter dat geen van deze arresten betrekking heeft op de fiscale discriminatie waarop hij nu de aandacht vestigt. Volgens hem bestaat er dus geen evidentie.

Tot slot merkt hij op dat zijn fractie het luik over de flexi-jobs als afzonderlijk wetsvoorstel had ingediend, zodat dit sneller en los van de discussie van het wetsontwerp door de Kamer zou kunnen worden behandeld.

De heer Lode Vereeck gaat vervolgens in op het tweede grote thema van zijn tussenkomst: het CAP en het gebruik van algoritmische risicomodellen binnen het kader van *money control*.

Hij benadrukt vooraf dat zijn opmerkingen niet voortkomen uit weerstand tegen de bestrijding van fiscale fraude. Integendeel, fiscale fraude is volgens hem diefstal en moet kordaat worden aangepakt. Zijn bedoeling is een robuuste wetgeving tot stand te brengen. In dat licht merkt hij op dat in de parlementaire debatten van de afgelopen weken nauwelijks aandacht is besteed aan het risico van bias in algoritmische systemen.

Hij licht kort toe wat onder algoritmische bias moet worden verstaan: een systematische vertekening in een model waardoor bepaalde groepen onevenredig nadelig worden behandeld. Deze vorm van bias is niet louter technisch, maar ook politiek en juridisch relevant, omdat zij kan leiden tot schending van het gelijkheidsbeginsel en tot discriminatie. Datamining die op geheime wijze gebeurt, maakt die ongelijke behandeling bovendien minder zichtbaar en daardoor moeilijker juridisch aan te vechten, tenzij de wet uitdrukkelijk voorziet in mechanismen om bias te detecteren en te corrigeren.

Als illustratie verwijst hij naar het bekende voorbeeld van *proxy bias* via het gebruik van postcodes. Hoewel juridisch op zichzelf legitiem, functioneren postcodes empirisch vaak als proxy voor etnische of sociaal-economische segregatie. Hetzelfde risico bestaat bij andere variabelen die op het eerste gezicht neutraal zijn.

De heer Vereeck formuleert vervolgens een reeks vragen aan de minister:

étabissements Horeca disposant ou non d'une caisse "blanche". Aucune discrimination n'a été constatée dans ces différents cas, et il en va de même pour l'examen des régimes transitoires applicables aux travailleurs passant à un emploi à quatre cinquièmes.

M. Vereeck souligne cependant qu'aucun de ces arrêts ne concerne la discrimination fiscale sur laquelle il attire l'attention. Selon lui, il n'existe donc aucune preuve à cet égard.

Enfin, il fait observer que son groupe avait présenté la partie relative aux flexi-jobs sous la forme d'une proposition de loi distincte, afin qu'elle puisse être examinée plus rapidement et indépendamment de la discussion du projet de loi devant la Chambre.

M. Lode Vereeck aborde ensuite le deuxième grand thème de son intervention: le PCC et l'utilisation de modèles de risque algorithmiques dans le cadre du *money control*.

Il commence par souligner que ses observations ne procèdent pas d'une résistance à la lutte contre la fraude fiscale. Au contraire, selon lui, la fraude fiscale est un vol et elle doit être combattue avec fermeté. Son objectif est de mettre en place une législation solide à cet égard. À cet égard, il souligne que les débats parlementaires des dernières semaines n'ont pratiquement pas porté sur le risque de biais des systèmes algorithmiques.

Il explique brièvement ce qu'il faut entendre par "biais algorithmique". Il s'agit d'une distorsion systématique d'un modèle qui désavantage certains groupes de manière disproportionnée. Ces biais ne sont pas seulement pertinents sur le plan technique, mais aussi sur les plans politique et juridique, car ils peuvent être à l'origine de violations du principe d'égalité et de discriminations. De plus, lorsque le *data mining* est effectué de manière confidentielle, cette inégalité de traitement est moins visible et elle est donc plus difficile à contester sur le plan juridique, sauf si la loi prévoit explicitement des mécanismes de détection et de correction de ces biais.

Pour illustrer son propos, l'intervenant cite le célèbre exemple du biais de substitution (*proxy bias*) lié à l'utilisation des codes postaux. Bien que leur usage soit juridiquement légitime, ceux-ci servent souvent, d'un point de vue empirique, de substitut pour la ségrégation ethnique ou socio-économique. Le même risque existe pour d'autres variables qui semblent neutres de prime abord.

M. Vereeck adresse ensuite une série de questions au ministre:

Hij vraagt om toe te lichten hoe wordt gegarandeerd dat het risicomodel – want *money control* is uiteindelijk een risicomodel – geen directe of indirecte discriminatie veroorzaakt, ook niet wanneer het gebruikmaakt van ogenschijnlijk legitieme variabelen die in de praktijk als *proxy* kunnen functioneren en zo toch indirect discriminerend uitpakken.

Hij vraagt tevens of de minister kan garanderen dat de variabelen die in het model worden opgenomen niet onbedoeld tot bias leiden, en welke mechanismen bestaan om systematisch te controleren of de resulterende risicoscores bepaalde groepen vaker of zwaarder treffen dan andere.

Daarnaast vraagt hij de minister om uit te leggen hoe biasdetectie en de noodzakelijke tegenmaatregelen – de zogenaamde *fairness metrics* – zijn ingebouwd in het *money control*-model of in de gebruikte modellen.

Verder wil de heer Vereeck weten welke maatregelen worden genomen om historische data, die per definitie historische bias kunnen bevatten, te screenen, aangezien dataminingmethoden patronen zoeken die grotendeels op historische informatie steunen.

Hij vraagt de minister of hij bereid is risicomodellen expliciet te testen op hun ongewenste effecten, met name bias en discriminatie, en – indien ja – wie die testen moet uitvoeren.

Aangezien de minister eerder verklaarde dat een intern team van de FOD Financiën naar valse positieven zoekt, vraagt hij of de minister ook bereid is een onafhankelijke toezichthouder aan te stellen – buiten zowel de FOD Financiën als de Nationale Bank van België – om modellen te screenen of zo nodig te schorsen wanneer bias wordt vastgesteld.

In dat verlengde vraagt hij of de minister bereid is biasbevindingen te documenteren en de volledige modeldocumentatie open te stellen zodat onafhankelijke onderzoekers, in het bijzonder academici, deze kunnen bestuderen.

De heer Vereeck maakt hierbij een korte zijsprong en stelt dat hij de oprichting van zo'n toezichthouder niet zou willen beperken tot fiscale bias, maar dat het volgens hem wenselijk zou zijn een algemene toezichthouder op algoritmisch overheidsgebruik te voorzien – dus niet alleen inzake fiscaliteit, maar voor alle algoritmes die door de overheid worden ingezet.

Il demande des précisions sur les dispositions qui seront prises pour garantir que le modèle de risque – le *money control* étant *in fine* un modèle de risque – ne provoquera aucune discrimination directe ou indirecte, même en cas d'utilisation de variables légitimes en apparence mais qui peuvent, en pratique, servir de substituts et se révéler indirectement discriminatoires.

Il demande également si le ministre peut garantir que les variables intégrées dans le modèle ne seront pas source de biais involontaires, et quels mécanismes permettent de vérifier systématiquement si les scores de risque visent certains groupes plus souvent ou plus fortement que d'autres.

Il demande également au ministre d'expliquer comment la détection des biais et les contre-mesures nécessaires – appelées *fairness metrics* – ont été intégrées dans le *money control* ou dans les modèles utilisés.

M. Vereeck s'enquiert ensuite des mesures prises pour contrôler les données historiques qui, par définition, peuvent contenir des biais historiques puisque les méthodes de *data mining* recherchent des schémas qui reposent en grande partie sur des informations historiques.

Il demande au ministre s'il est prêt à tester explicitement les modèles de risque en fonction de leurs effets indésirables, comme les biais et la discrimination, et d'indiquer – dans l'affirmative – par qui ces tests seront effectués.

Étant donné que le ministre a précédemment déclaré qu'une équipe interne du SPF Finances recherchait les faux positifs, l'intervenant demande si le ministre est également disposé à désigner une autorité de contrôle indépendante – extérieure au SPF Finances et à la Banque nationale de Belgique – pour examiner les modèles, voire pour les suspendre en cas de biais constatés.

À cet égard, il demande si le ministre est prêt à documenter les constats relatifs aux biais et à publier toute la documentation relative au modèle afin que des chercheurs indépendants, notamment des universitaires, puissent l'étudier.

M. Vereeck fait brièvement observer au passage qu'il ne souhaite pas que les compétences de cette autorité de contrôle soient limitées aux biais fiscaux, et qu'il serait selon lui souhaitable de mettre en place une autorité de contrôle générale qui contrôlerait l'usage d'algorithmes par les pouvoirs publics, et donc pas seulement en matière fiscale, mais pour tous les algorithmes déployés par les autorités publiques.

Vervolgens keert hij terug naar de concrete risico-factoren. Er is eerder gesproken over het gebruik van postcodevariabelen, maar de vraag blijft hoe er wordt voorkomen dat andere variabelen – zoals cashgebruik, mobiliteit, buitenlandse transacties of sectoractiviteit – onbedoeld tot indirecte discriminatie leiden. Hij verwijst hierbij expliciet naar bepaalde beroepsgroepen – zelfstandigen, horecapersoneel, transporteurs of marktkramers – die door dergelijke variabelen disproportioneel geraakt zouden kunnen worden.

Daarnaast wijst de spreker op het bestaan van databron-bias en historische bias. Hij vraagt of er reeds protocollen bestaan om dit soort bias systematisch op te sporen, wanneer deze voortkomt uit datakwaliteitsproblemen of historische onnauwkeurigheden in databanken.

Daarbovenop bestaat er modelbias, waarbij bepaalde algoritmen inherente tendensen hebben die ongelijkheden kunnen versterken. Hij geeft voorbeelden:

- *boostingmodellen* die kleine verschillen systematisch uitvergroten;
- neurale netwerken die complexe correlaties kunnen genereren met onevenredige impact;
- *random forests* die groepen met weinig data onvoldoende representeren.

De heer Vereeck benadrukt dat daarom niet alleen de data en de parameters, maar ook de modelkeuze bepalend is voor het risico op discriminatie. Zijn vraag aan de minister luidt dus: welke type modellen worden binnen *money control* gebruikt, en welke stappen worden gezet om modelbias te vermijden of te corrigeren?

Hij erkent dat dit geen eenvoudige opdracht is, omdat complexe modellen bias kunnen verhullen.

Daarom vraagt hij ook welke maatregelen worden genomen om causale bias op te sporen en te verwijderen, dus situaties waarin foutieve aannames over oorzaak en gevolg in het model sluipen.

Vervolgens vraagt hij hoe wordt voorkomen dat risico-indicatoren in het model worden opgenomen die geen logisch of causaal verband houden met fraude. Datamining werkt immers met correlaties, niet met causaliteit, en

L'intervenant revient ensuite sur les facteurs de risque concrets. Il a déjà été question de l'utilisation de variables liées au code postal, mais la question qui demeure est celle de savoir comment éviter que d'autres variables – telles que l'utilisation d'argent liquide, la mobilité, les transactions à l'étranger ou l'activité sectorielle – causent involontairement des discriminations indirectes. Il renvoie explicitement à certaines catégories professionnelles pouvant être disproportionnellement affectées par de telles variables – indépendants, personnel de l'horeca, transporteurs ou marchands ambulants.

L'intervenant attire également l'attention sur l'existence de biais dans les sources de données et de biais historiques. Il demande si des protocoles ont déjà été mis au point pour détecter systématiquement les biais de ce type, qui surviennent lorsque les données sont affectées par une qualité insuffisante ou par des inexactitudes historiques.

S'y ajoute le biais de modèle, certains algorithmes ayant tendance à renforcer les inégalités. Il en donne quelques exemples:

- les *modèles de boosting* qui amplifient systématiquement les différences minimales;
- les réseaux neuronaux qui peuvent générer des corrélations complexes avec un impact disproportionné;
- les *forêts d'arbres décisionnels* qui représentent insuffisamment les groupes pour lesquels peu de données sont disponibles.

M. Vereeck souligne que ce ne sont donc pas seulement les données et les paramètres, mais aussi le choix du modèle qui déterminent le risque de discrimination. Sa question au ministre est donc la suivante: quels sont les types de modèles utilisés dans le cadre de *money control*, et quelles sont les mesures prises pour éviter ou corriger le biais de modèle?

Il reconnaît qu'il ne s'agit pas d'une tâche simple, car les modèles complexes peuvent masquer les biais existants.

C'est pourquoi il demande également quelles mesures sont prises pour détecter et éliminer le biais causal, à savoir les situations dans lesquelles certaines hypothèses erronées sur la relation de cause à effet s'introduisent dans le modèle.

Ensuite, il demande comment il est prévu d'éviter d'intégrer dans le modèle des indicateurs de risque n'ayant aucun lien logique ni causal avec la fraude. L'exploration de données fonctionne en effet sur la base

hij wil weten hoe wordt gegarandeerd dat parameters niet leiden tot schijnverbanden die burgers onterecht verdacht maken.

Daarnaast vraagt hij welke maatregelen verzekeren dat ambtenaren zich bewust zijn van biasrisico's. De minister verwees eerder naar technische opleidingen, maar de heer Vereeck vraagt of ambtenaren ook sociaal-wetenschappelijke vorming krijgen om bias te herkennen en te vermijden.

Hij vraagt eveneens hoe wordt voorkomen dat externe partijen – zoals consultants of softwareleveranciers – causale aannames introduceren die niet democratisch getoetst zijn.

Verder wil de spreker weten hoe de administratie zal omgaan met situaties waarin risicomodellen disproportionele effecten signaleren die operationeel misschien wenselijk lijken, en welke meldings- en documentatieplicht de administratie heeft bij biasincidenten, inclusief gevallen waarin foutpositieve patronen bepaalde bevolkingsgroepen onevenredig vaak aanduiden.

Tot slot vraagt de heer Vereeck de minister hoe bias wordt opgelost wanneer ze wordt vastgesteld. Hij vraagt specifiek of de minister bereid is te werken met *random sampling* – willekeurige steekproeven die, net omdat ze willekeurig zijn, per definitie niet onderhevig zijn aan bias.

Hij vervolgt dat hij van collega's uit de meerderheid de reactie hoorde dat het systeem eerst moest worden ingevoerd en dat men eventuele problemen later wel zou bekijken. Voor de heer Vereeck is dat een onaanvaardbare benadering. Volgens hem voert de regering zo een fiscaal experiment uit zonder voorafgaand inzicht in de mogelijke maatschappelijke impact. Hierdoor zouden volgens hem burgers het risico lopen slachtoffer te worden van een gebrekkig ontworpen fiscaal detectiemodel, met potentieel zware sociale gevolgen. Dat acht hij onzorgvuldig en asociaal beleid.

Hij verwijst in dat verband naar wetenschappelijke literatuur, met name het boek *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* van Cathy O'Neill (2016), waarin wordt aangetoond dat voorspellende modellen in een sociale context vrijwel altijd tot discriminatie leiden, tenzij ze worden gereguleerd.

de correlaties en non d'une causalité, et il souhaite savoir comment il sera garanti que les paramètres ne conduiront pas à des corrélations "fantômes", qui rendraient certains citoyens suspects de manière injustifiée.

Il s'interroge par ailleurs sur les mesures prévues pour garantir que les fonctionnaires aient conscience des risques de biais. Le ministre avait précédemment fait référence à des formations techniques, mais M. Vereeck demande si les fonctionnaires reçoivent également une formation en sciences sociales afin de reconnaître et d'éviter les biais.

Il demande également comment il sera évité que des parties externes – telles que des consultants ou des fournisseurs de logiciels – introduisent des hypothèses causales qui n'ont pas été soumises à un contrôle démocratique.

Par ailleurs, l'intervenant souhaite savoir comment l'administration traitera les situations dans lesquelles les modèles de risque signalent des effets disproportionnés qui peuvent sembler opérationnellement souhaitables, et quelle obligation de signalement et de documentation incombe à l'administration en cas d'incidents liés aux biais, y compris dans les cas où des schémas de faux positifs désignent certains groupes de population avec une fréquence disproportionnée.

Enfin, M. Vereeck demande au ministre comment les biais seront corrigés lorsqu'ils seront détectés. Il demande spécifiquement si le ministre est disposé à recourir à des *random samplings*, à savoir des échantillons aléatoires qui, précisément en raison de cette caractéristique, ne sont par définition pas soumis aux biais.

Il poursuit en soulignant la réaction de certains collègues de la majorité, selon lesquels le système devrait d'abord être mis en œuvre avant d'examiner les problèmes qui surviendront le cas échéant. Pour M. Vereeck, cette manière de procéder serait inacceptable. Selon lui, le gouvernement mènerait ainsi une expérience fiscale sans connaître au préalable son impact potentiel sur la société. De ce fait, les citoyens courraient, selon lui, le risque de devenir victimes d'un modèle de détection fiscale imparfait pouvant potentiellement avoir des conséquences sociales importantes. Il s'agirait là d'une politique irréfléchie et antisociale.

Il renvoie à cet égard à la littérature scientifique, notamment à l'ouvrage *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* de Cathy O'Neill (2016), qui démontre que les modèles prédictifs dans un contexte social donnent presque toujours lieu à des discriminations, sauf lorsqu'ils sont régulés.

De heer Lode Vereeck vervolgt zijn tussenkomst met opmerkingen over de noodzaak om bias te corrigeren door middel van *fairness*mechanismen. Hij vraagt de minister te bevestigen dat *fairness* en non-discriminatie minstens even zwaar moeten doorwegen als efficiëntie bij de ontwikkeling en toepassing van risicomodelen. Bias moet volgens hem worden gecounterd door *fairness*maatstaven, en daarom wenst hij te vernemen welke *fairness metrics* momenteel zijn ingebouwd in het dataminingmodel voor fiscale controles. Daarnaast vraagt hij welke garanties er bestaan dat het model systematisch op *fairness* wordt gecontroleerd bij elke update of bij elke toevoeging van nieuwe gegevens.

Verder informeert hij of de minister bereid is verplichte *fairness audits* in te voeren voor alle dataminingmodellen, en of de resultaten daarvan openbaar zullen worden gemaakt. Hij vraagt ook hoe wordt gegarandeerd dat *fairness* testen worden uitgevoerd op gekoppelde datasets, waarin de foutenmarges en datakwaliteit uiteen kunnen lopen. En vooral: zal die *fairness* analyse worden uitgevoerd voor de bouw – of in dit geval de implementatie – van het dataminingmodel, dus *ex ante*, om problemen te voorkomen? Of worden de valse positieven en valse negatieven pas achteraf, *ex post*, beoordeeld, uitgesplitst naar ratio's per groep? En indien daarbij ongelijkheden worden vastgesteld, worden de modellen dan opnieuw getraind? Of gebeurt de beoordeling uitsluitend achteraf, via een toetsing door onafhankelijke auditors of eventueel door een rechtbank?

Hij verwijst vervolgens naar de hoge kans op valse positieven in fiscale datamining, wat volgens hem inherent is aan het feit dat de prevalentie van effectieve fraude zeer laag is.

De heer Vereeck gaat daarna in op het fenomeen *function creep*, een term uit de literatuur die verwijst naar het geleidelijke uitbreiden van systemen of technologieën naar doeleinden waarvoor zij oorspronkelijk niet waren bedoeld. Hij herinnert eraan dat dit juridisch problematisch is omdat het de vereiste van doelbinding, zoals vastgelegd in artikel 5 van de GDPR, onder druk zet.

Volgens hem zijn er vandaag al tekenen van *function creep* zichtbaar: het gebruik van het CAP, dat bij zijn oorspronkelijke ontwerp bedoeld was op gerichte fraudeopsporing, wordt nu uitgebreid naar massale en probabilistische risicodetectie. Hij verwijst in dit verband naar waarschuwingen van collega Wouter Vermeersch in de vorige legislatuur.

M. Lode Vereeck poursuit son intervention par des observations relatives à la nécessité de corriger les biais au moyen de mécanismes d'équité. Il demande au ministre de confirmer que l'équité et la non-discrimination auront un poids au moins équivalent à celui de l'efficacité dans le développement et l'application des modèles de risque. Selon lui, les biais doivent être contrebalancés par des critères d'équité, et il souhaite donc savoir quels paramètres d'équité sont actuellement intégrés dans le modèle d'exploration de données relatif aux contrôles fiscaux. Il demande également quelles garanties existent que l'équité du modèle fasse systématiquement l'objet d'une évaluation, à chaque mise à jour ou à chaque ajout de nouvelles données.

L'intervenant demande par ailleurs si le ministre est disposé à instaurer des audits obligatoires visant à évaluer l'équité de l'ensemble des modèles d'exploration de données, et si leurs résultats seront rendus publics. Il s'enquiert aussi des garanties que les ensembles de données liés, où les marges d'erreur et la qualité des données peuvent être variables, seront soumis à des tests d'équité. Et surtout: cette analyse de l'équité sera-t-elle réalisée avant l'élaboration – ou, dans le cas présent, l'implémentation – du modèle d'exploration de données, donc *ex ante*, afin de prévenir toute apparition de difficultés? Ou bien l'évaluation relative aux faux positifs et aux faux négatifs n'aura-t-elle lieu qu'*a posteriori*, donc *ex post*, après ventilation de ceux-ci en ratios par groupe? Au cas où des inégalités seraient constatées, les modèles seront-ils réentraînés? Ou bien l'évaluation se fera-t-elle uniquement *a posteriori*, par le biais d'un contrôle réalisé par des auditeurs indépendants, voire par un tribunal le cas échéant?

Le membre renvoie ensuite à la forte probabilité que l'exploration de données en matière fiscale génère des faux positifs, ce qui, selon lui, est inhérent à la faible prévalence de la fraude effective.

M. Vereeck aborde ensuite le phénomène du détournement de fonction, un terme issu de la littérature qui désigne l'élargissement progressif de systèmes ou de technologies à des finalités pour lesquelles ils n'étaient pas conçus au départ. Il rappelle que ce phénomène pose un problème juridique dès lors qu'il met en péril l'exigence relative à la finalité du traitement, prévue par l'article 5 du RGPD.

Selon lui, des signes de détournement de fonction apparaissent déjà aujourd'hui: l'utilisation du PCC, qui, lors de sa conception initiale, était destiné à la détection ciblée de cas de fraude, est désormais étendue à une détection massive et probabiliste des risques. Il renvoie à cet égard aux avertissements formulés par son collègue Wouter Vermeersch sous la législature précédente.

De heer Vereeck vraagt de minister hoe toekomstige vormen van *function creep* kunnen worden voorkomen. Hoe wordt wettelijk gegarandeerd dat gegevens niet worden hergebruikt voor doeleinden waarvoor geen wettelijke basis bestaat? Hoe wordt vermeden dat geautomatiseerde dossiersselectie uitgroeit tot geautomatiseerde beslissingen over fraudevaststelling en sancties? Hij vraagt uitdrukkelijk bevestiging dat zulke autonome beslissingen nooit zullen worden toegestaan en wil weten welke mechanismen dit effectief waarborgen.

Daarnaast wijst hij erop dat *function creep* niet enkel ontstaat via nieuwe grote wetten, maar ook via kleine technische uitbreidingen. Hij informeert daarom naar de preventieve maatregelen die worden voorzien om dergelijke sluipende uitbreidingen te vermijden.

Datamining zoekt immers niet enkel naar fouten maar naar patronen, en volgens hem moet worden beseft dat *money control* in essentie gaat over belastingrisicogedrag en niet over belastingfraude.

Vervolgens staat de heer Vereeck stil bij mogelijke risico's die voortvloeien uit datakoppelingen tussen het CAP, het *datawarehouse* van de FOD Financiën en eventueel andere databanken. Hij vraagt welke maatregelen worden genomen om te vermijden dat datakoppelingen die vandaag operationeel noodzakelijk worden geacht, morgen worden uitgebreid naar nieuwe beleidsdoeleinden. Hij vraagt eveneens aan de minister hoe wordt gewaarborgd dat databanken die voor andere beleidsdomeinen werden ontworpen, niet via *money control* worden ingezet voor fiscale surveillance. Hij verwijst naar een passage in het regeerakkoord waarin bijkomende databankkoppelingen worden vermeld, en vraagt hoe wordt gegarandeerd dat fiscale datamining niet wordt toegepast op databanken die oorspronkelijk voor andere beleidsdomeinen zijn ontwikkeld.

Hij wenst eveneens te vernemen hoe wordt voorkomen dat gecombineerde *datasets* met uiteenlopende definities, foutenmarges en actualiteit leiden tot foutieve conclusies binnen *money control*.

Hoewel IT-diensten formeel zijn gescheiden van fiscale diensten, vraagt hij welke wettelijke garanties ervoor zorgen dat IT-teams of analisten geen nieuwe koppelingen kunnen doorvoeren zonder voorafgaande democratische en juridische toetsing. De vraag is volgens hem essentieel: welke mechanismen voorkomen dat

M. Vereeck demande au ministre comment les diverses formes de détournement de fonction pourront être évitées à l'avenir. Quelles sont les garanties juridiques qui feront obstacle à la réutilisation de données pour des finalités non régies par une base légale? Comment sera-t-il évité que la sélection automatisée de dossiers ne se transforme en décisions automatisées concernant la constatation de cas de fraude et les sanctions? Il demande expressément confirmation que de telles décisions autonomes ne seront jamais autorisées et souhaite savoir quels mécanismes feront office de garantie effective à cet égard.

Il souligne en outre que le détournement de fonction n'apparaît pas seulement lorsque de nouvelles lois de grande ampleur sont adoptées, mais également en cas de petites extensions techniques. Il s'informe dès lors des mesures préventives prévues pour éviter de telles extensions insidieuses.

En effet, l'exploration de données ne recherche pas uniquement les erreurs mais aussi les schémas, et selon lui, il faut prendre conscience du fait que *money control* porte essentiellement sur les comportements à risque en matière fiscale et non sur la fraude fiscale.

M. Vereeck s'arrête ensuite sur les risques qui pourraient résulter des couplages de données entre le PCC, le *datawarehouse* du SPF Finances et d'autres banques de données éventuelles. Il s'enquiert des mesures qui seront prises pour éviter que les couplages de données qui sont aujourd'hui jugés nécessaires d'un point de vue opérationnel soient étendus demain à de nouveaux objectifs politiques. Il demande également au ministre comment il peut garantir que les banques de données conçues pour d'autres domaines stratégiques ne seront pas détournées à des fins de surveillance fiscale par le biais du *money control*. Il renvoie à un passage de l'accord de gouvernement évoquant des couplages supplémentaires de banques de données et demande comment on peut garantir que le *data mining* fiscal ne sera pas appliqué à des banques de données initialement développées pour d'autres domaines stratégiques.

Il demande également comment on pourra éviter que des ensembles de données combinés présentant des définitions, des marges d'erreur et des actualités divergentes n'aboutissent à des conclusions erronées dans le cadre du *money control*.

Bien que les services informatiques soient formellement séparés des services fiscaux, l'intervenant demande dans quelle mesure la loi a prévu des garanties pour empêcher les équipes informatiques ou les analystes d'effectuer de nouveaux couplages sans contrôle démocratique et juridique préalable. La question est essentielle à ses

ambtenaren – zowel binnen de de fiscale administratie als binnen de IT-diensten – nieuwe koppelingen kunnen implementeren zonder de voorafgaande parlementaire goedkeuring?

De heer Lode Vereeck wijst vervolgens op een bijkomend fenomeen dat volgens hem tot op heden nog niet aan bod is gekomen: het zogenaamde *chilling effect*. Dat begrip verwijst naar gedragsaanpassing die ontstaat door de vrees om permanent te worden geobserveerd of gemonitord.

Volgens de heer Vereeck is dat precies wat zich kan voordoen wanneer de overheid op grote schaal datamining toepast. Zodra gegevens in algoritmische systemen terechtkomen, zo stelt hij, wordt in de praktijk iedereen potentieel verdacht. Het staat volgens hem buiten kijf dat wetten moeten worden gehandhaafd en dat controles noodzakelijk zijn, maar wanneer burgers de indruk krijgen dat de overheid permanent hun gedrag analyseert, hun financiële gegevens monitort en profielscores bijhoudt, kan dat schadelijke gevolgen hebben voor het vertrouwen in overheid en samenleving. Hij verwijst hierbij naar het werk van professor Wim Moesen.

Volgens de heer Vereeck ondermijnt een dergelijke permanente surveillance niet alleen het vertrouwen in instellingen, maar ook de innovatiebereidheid, het nemen van economische risico's en de vrijwillige fiscale naleving. Waar vertrouwen de basis vormt van de democratische legitimiteit, verschuift bij een vorm van permanente financiële surveillance die relatie van vertrouwen naar wantrouwen.

De spreker wijst erop dat fiscale datamining een financieel *chilling effect* kan veroorzaken: burgers passen hun economisch gedrag mogelijk aan, vermijden bepaalde transacties of ondernemen minder uit vrees dat hun financiële profielen als afwijkend of risicovol worden beschouwd.

Hij benadrukt dat dit niet louter een randverschijnsel is, maar een kernprobleem dat uitgebreid in de literatuur wordt beschreven. Hij vergelijkt het fenomeen met snelheidscontroles: controles die de verkeersveiligheid bevorderen worden maatschappelijk aanvaard, maar controles die worden ervaren als instrumenten om de begroting te spijzen roepen maatschappelijke weerzin op.

De heer Vereeck richt vervolgens een aantal vragen aan de minister.

Ten eerste vraagt hij of de minister bekend is met het concept *chilling effect* en of dit fenomeen op enig moment in overweging is genomen bij de bespreking

yeux: Quels mécanismes a-t-on prévus pour empêcher les agents – de l'administration fiscale et des services informatiques – d'établir de nouveaux couplages sans l'accord préalable du Parlement?

M. Lode Vereeck épingle ensuite un phénomène supplémentaire qui, selon lui, n'a pas encore été abordé: l'effet de dissuasion (*chilling effect*). Cette notion désigne un changement de comportement dicté par la crainte d'être observé ou surveillé en permanence.

Selon M. Vereeck, c'est précisément ce qui pourra arriver si le *data mining* est appliqué à grande échelle par les pouvoirs publics. Il indique que dès que des données entrent dans les systèmes algorithmiques, tout le monde devient un suspect potentiel en pratique. L'intervenant ajoute que s'il ne fait aucun doute que les lois doivent être appliquées et que les contrôles sont nécessaires, lorsque les citoyens ont le sentiment que les pouvoirs publics analysent leur comportement, surveillent leurs données financières et enregistrent leurs scores de profil en permanence, cela peut éroder leur confiance dans les pouvoirs publics et dans la société. Il renvoie à cet égard aux travaux du professeur Wim Moesen.

M. Vereeck estime que cette surveillance permanente sape non seulement la confiance dans les institutions, mais aussi la volonté d'innover, la prise de risques économiques et le respect spontané des obligations fiscales. Alors que la confiance constitue le fondement de la légitimité démocratique, une forme de surveillance financière permanente transforme cette relation de confiance en méfiance.

L'intervenant souligne que le *data mining* fiscal pourrait avoir un effet dissuasif sur le plan financier: les citoyens pourraient modifier leur comportement économique, éviter certaines transactions ou réduire leur volonté d'entreprendre par crainte que leur profil financier soit considéré comme anormal ou risqué.

Il souligne qu'il ne s'agit pas simplement d'un épiphénomène, mais d'un problème fondamental largement décrit dans la littérature. Il compare ce phénomène aux contrôles de vitesse: les contrôles qui favorisent la sécurité routière sont socialement admis, mais les contrôles perçus comme des instruments destinés à faire rentrer de l'argent dans les caisses suscitent de la réticence.

M. Vereeck pose ensuite plusieurs questions au ministre.

Il demande d'abord si le ministre connaît le concept de l'effet de dissuasion (*chilling effect*) et si ce phénomène a été pris en considération au cours de la discussion ou

of beoordeling van *money control*: bijvoorbeeld bij de onderhandelingen over het regeerakkoord of tijdens interkabinettenwerkgroepen. Hoe belangrijk acht de minister dit?

Ten tweede vraagt hij of de regering onderzoek heeft laten verrichten naar de psychologische impact op burgers, hoe moeilijk die ook te meten valt, en naar de mogelijke gedragsaanpassing van burgers die niet uit fraude-intentie, maar uit angst voortvloeit. Hij verwijst opnieuw naar professor Moesen, die waarschuwt dat het vertrouwen in de overheid kan worden aangetast wanneer burgers het gevoel hebben dat hun financiële gedrag voortdurend wordt geanalyseerd.

Tot slot vraagt de heer Vereeck welke concrete stappen de minister wil zetten (1) om te voorkomen dat burgers zich gevisieerd of onterecht verdacht gemaakt voelen, en (2) om te vermijden dat *money control* leidt tot zogeheten *normatieve drift*, waarbij burgers hun gedrag beperken op manieren die niet wettelijk vereist zijn, louter uit vrees voor fiscale misinterpretatie. Welke maatregelen zullen dus worden genomen om dergelijke *chilling effects* te vermijden?

Vervolgens benadrukt de heer Lode Vereeck dat hij persoonlijk een groot vertrouwen heeft in de fiscale administratie. Hij erkent dat dit een anekdotische ervaring is, maar dat zijn eigen dossiers – hoewel het resultaat niet steeds aangenaam was – correct werden afgehandeld.

Net daarom, zo stelt hij, is het van belang te waken over het vertrouwen dat burgers in de fiscale administratie moeten kunnen blijven hebben.

Hij vraagt hoe de minister kan garanderen dat systemen zoals *money control* dat vertrouwen niet ondermijnen. Hoe wordt ervoor gezorgd dat datamining niet onbedoeld leidt tot een cultuur waarin burgers structureel als potentiële fraudeurs worden beschouwd?

De heer Vereeck verwijst hierbij naar het concept van vrijwillige fiscale naleving. Die ontstaat volgens hem uit vertrouwen en niet uit angst. Hij vraagt dan ook welke concrete maatregelen de minister neemt om te vermijden dat datamining leidt tot een daling van die vrijwillige naleving. Anders gezegd: hoe wordt gewaarborgd dat fiscale moraal en fiscale ethiek – de bereidheid om spontaan en correct aan fiscale verplichtingen te voldoen – centraal blijven staan in het fiscale beleid, ondanks de toenemende datagedreven controlemechanismen?

de l'évaluation du *money control*, par exemple lors des négociations sur l'accord de gouvernement ou dans les groupes de travail intercabineaux. Quelle importance le ministre lui accorde-t-il?

Il demande ensuite si le gouvernement a fait étudier ses effets psychologiques sur les citoyens, si difficiles soient-ils à mesurer, et les changements de comportement qu'il peut induire chez les citoyens, non pas en raison d'une intention frauduleuse, mais sous l'effet de la peur. Il renvoie à nouveau au professeur Moesen, qui met en garde contre le fait que la confiance dans les pouvoirs publics peut être ébranlée lorsque les citoyens ont le sentiment que leur comportement financier est analysé en permanence.

Enfin, M. Vereeck demande au ministre quelles mesures concrètes il envisage de prendre pour éviter, d'une part, que les citoyens se sentent visés ou injustement soupçonnés, et, d'autre part, que le *money control* entraîne une "dérive normative" (*normative drift*), c'est-à-dire pour éviter que les citoyens brident leurs comportements non pas pour répondre à des prescriptions légales mais bien par crainte d'une mauvaise interprétation fiscale. Quelles mesures va-t-il donc prendre pour éviter ces effets de dissuasion?

M. Lode Vereeck souligne ensuite qu'il place personnellement une grande confiance dans l'administration fiscale. Il admet que son expérience relève de l'anecdote, mais souligne que – même si le résultat n'a pas toujours été agréable – ses propres dossiers ont été traités correctement.

C'est précisément pour cette raison qu'il pense qu'il est essentiel de veiller à ce que les citoyens puissent continuer à avoir confiance dans l'administration fiscale.

Il demande comment le ministre pourra garantir que les systèmes tels que le *money control* ne sapent pas cette confiance. Comment s'assurer que le *data mining* n'aboutisse pas involontairement à une culture dans laquelle les citoyens sont considérés par leurs institutions comme des fraudeurs potentiels?

M. Vereeck évoque à cet égard le concept de respect spontané des obligations fiscales, qui, selon lui, découle de la confiance et non de la peur. Il demande donc une fois encore au ministre de lui préciser les mesures concrètes envisagées pour éviter que le *data mining* entraîne une diminution de ce respect spontané. En d'autres termes, comment garantir que la morale et l'éthique fiscales – la disposition à se conformer spontanément et correctement aux obligations fiscales – restent au cœur de la politique fiscale, malgré la multiplication des mécanismes de contrôle basés sur les données?

Daarnaast vraagt hij aandacht voor de perceptie van overcontrole, een fenomeen dat bij burgers én ondernemingen kan ontstaan, en dat in sommige sectoren al sterk aanwezig is. Hij vreest dat *money control* die perceptie kan versterken. Daarom vraagt hij welke maatregelen worden genomen of nog zullen worden ingevoerd om dat gevoel van overmatige controle te temperen en transparantie te vergroten.

Verder vraagt de heer Vereeck welke mechanismen voorzien zijn voor burgers die ten onrechte of foutief worden geselecteerd door een dataminingmodel. Zij krijgen immers wel een fiscale controle opgelegd, ook indien zij uiteindelijk volledig in regel blijken te zijn. Bestaan er garanties dat deze burgers op de een of andere manier kunnen worden gecompenseerd of gerehabiliteerd?

Tot slot vraagt hij de minister te bevestigen dat fiscale handhaving niet uitsluitend repressief wordt benaderd, maar ook ondersteunend blijft.

De heer Lode Vereeck vraagt vervolgens bijkomende toelichting over de kwaliteitscontroles op de gegevens in het CAP. Hij wenst te vernemen welke mechanismen bestaan voor foutdetectie en het opsporen van ontbrekende waarden.

Hij benadrukt dat deze vraag essentieel is om te garanderen dat de gegevens die in *money control* worden gebruikt correct, actueel en volledig zijn vóór zij in dataminingmodellen worden opgenomen.

De heer Vereeck verwijst naar de informatie in het CAP die om de zes maanden wordt geüpdatet. Hij vraagt bevestiging of dit correct is en welke risico's bestaan wanneer analyses worden uitgevoerd op gegevens die vijf maanden oud kunnen zijn. Indien de update niet in real time gebeurt, vraagt hij hoe wordt voorkomen dat burgers geselecteerd worden op basis van verouderde of verkeerd geregistreerde bankgegevens.

Daarnaast vraagt hij of de minister kan garanderen dat verschillen in datadefinities tussen databanken – enerzijds het CAP en anderzijds de gegevens van de FOD Financiën – niet leiden tot foutieve conclusies.

Verder vraagt hij naar de procedures voor het snel corrigeren van onjuiste of onvolledige data. Worden burgers op de hoogte gebracht wanneer hun gegevens foutief blijken te zijn, of verwacht de administratie (CAP en FOD Financiën) dat burgers zelf melding moeten maken van fouten? Hoe gaat de administratie concreet

Il attire également l'attention sur la perception de contrôle excessif, un phénomène qui peut se manifester chez les citoyens et dans les entreprises, et qui est déjà très présent dans certains secteurs. Il craint que *money control* ne renforce cette perception. C'est pourquoi il demande quelles mesures sont ou seront prises pour atténuer ce sentiment de contrôle excessif et accroître la transparence.

M. Vereeck demande également quels sont les mécanismes prévus pour les citoyens qui seront sélectionnés à tort ou de manière erronée par un modèle de *data mining*. En effet, ils feront l'objet d'un contrôle fiscal, même s'ils s'avèrent finalement être parfaitement en règle. Existe-t-il des garanties que ces citoyens puissent bénéficier de compensations ou être réhabilités d'une manière ou d'une autre?

Enfin, il demande au ministre de confirmer que l'application de la législation fiscale ne sera pas uniquement répressive et que les contribuables continueront aussi à bénéficier d'une aide.

M. Lode Vereeck demande ensuite des explications complémentaires sur les contrôles de la qualité des données figurant dans le PCC. Il souhaite connaître les mécanismes existants pour détecter les erreurs et les valeurs manquantes.

Il souligne que cette question est essentielle pour garantir que les données utilisées dans le cadre de *money control* soient correctes, à jour et complètes avant d'être intégrées dans des modèles de *data mining*.

M. Vereeck fait référence aux informations contenues dans le PCC, qui sont mises à jour tous les six mois. Il demande confirmation de l'exactitude de ces informations et souhaite connaître les risques liés à l'analyse de données pouvant dater de cinq mois. Si la mise à jour n'est pas effectuée en temps réel, il demande comment éviter que des citoyens soient sélectionnés sur la base de données bancaires obsolètes ou incorrectement enregistrées.

Il demande également au ministre s'il peut garantir que les différences entre banques de données – d'une part, le PCC et, d'autre part, les données du SPF Finances – en matière de définition des données ne conduiront pas à des conclusions erronées.

Il s'interroge également sur les procédures mises en place pour corriger rapidement les données erronées ou incomplètes. Les citoyens sont-ils informés lorsque leurs données s'avèrent incorrectes, ou bien l'administration (le PCC et le SPF Finances) attend-elle des citoyens qu'ils signalent eux-mêmes les erreurs? Comment

om met meldingen van burgers dat hun gegevens onjuist verwerkt zijn?

Met betrekking tot datakwaliteit vraagt de heer Vereeck ook verduidelijking over de statistische methoden die worden gebruikt om onschuldige outliers – uitzonderlijke maar volledig legitieme financiële transacties – te onderscheiden van echte indicaties van fraude. Hoe wordt vermeden dat zulke outliers automatisch en onterecht als risicovol worden gecapteerd door *money control*?

Hij vraagt tevens garanties dat de gebruikte risico-modellen niet overgevoelig zijn aan kleine variaties in data, wat kan wijzen op onvoldoende kalibratie en tot foutieve selecties kan leiden.

Tot slot vraagt de spreker hoe de administratie omgaat met veranderende definities van variabelen in de tijd, en op welke manier inconsistenties in de berekeningen van fiscaal risicogedrag worden vermeden wanneer dergelijke definities evolueren.

Daarnaast merkt de heer Vereeck op dat hij nog omvangrijke vragen heeft over de technische beveiliging, met name inzake hacking, datalekken en de robuustheid van de CAP-infrastructuur, maar dat hij die voor dit moment terzijde laat om zich te concentreren op het model zelf: *money control*.

Hij wijst erop dat diverse personen met wie hij recent overlegde hem dezelfde fundamentele vraag stelden: hoe wordt de modelprestatie van *money control* gemeten? Hoe wordt de nauwkeurigheid en betrouwbaarheid van dit model geëvalueerd?

Daarbij komt een tweede, cruciale vraag: maakt de FOD Financiën bij fiscale datamining gebruik van slechts één model, of betreft het een geheel van modellen dat parallel of sequentieel wordt toegepast op de gegevens van het CAP? Anders gezegd: bestaat *money control* uit één enkel dataminingmodel, of gaat het om een verzameling van modellen, technieken of algoritmes die in combinatie opereren?

Bovendien onderstreept de heer Vereeck dat er verschillende dataminingtechnieken bestaan, en dat – zo benadrukken de betrokken juridische experts – elke specifieke vorm van datamining afzonderlijk moet worden toegelicht en in feite een eigen regulerend kader vereist.

Daarom herhaalt hij zijn vraag: gaat het om één model of om meerdere modellen? En indien het om meerdere modellen gaat, op welke basis wordt bepaald welk model

l'administration traite-t-elle concrètement les signalements des citoyens concernant le traitement incorrect de leurs données?

À l'égard de la qualité des données, M. Vereeck demande également des précisions sur les méthodes statistiques utilisées pour distinguer les valeurs atypiques innocentes – des transactions financières exceptionnelles mais tout à fait légitimes – des véritables indices de fraude. Comment éviter que ces valeurs atypiques soient automatiquement et injustement considérées comme étant à risque par *money control*?

Il demande également des garanties que les modèles de risque utilisés ne soient pas trop sensibles aux petites variations dans les données, ce qui pourrait indiquer un étalonnage insuffisant et conduire à des sélections erronées.

Enfin, l'intervenant demande comment l'administration gère le changement des définitions de variables au fil du temps et comment elle évite les incohérences dans les calculs des comportements fiscaux à risque lorsque ces définitions évoluent.

Par ailleurs, M. Vereeck fait observer qu'il a encore de nombreuses questions concernant la sécurité technique, notamment en matière de piratage, de fuites de données et de robustesse de l'infrastructure du PCC, mais qu'il les met de côté pour l'instant afin de se concentrer sur le modèle lui-même: *money control*.

Il souligne que plusieurs personnes avec lesquelles il s'est récemment entretenu lui ont posé la même question fondamentale: comment mesure-t-on la performance du modèle *money control*? Comment évalue-t-on sa précision et sa fiabilité?

Une deuxième question cruciale s'y ajoute: le SPF Finances utilise-t-il un seul modèle pour le *data-mining* fiscal, ou s'agit-il d'un ensemble de modèles qui sont appliqués en parallèle ou de manière séquentielle aux données du PCC? En d'autres termes, *money control* consiste-t-il en un seul modèle de *data mining*, ou bien est-il question d'un ensemble de modèles, de techniques ou d'algorithmes qui fonctionnent de manière combinée?

En outre, M. Vereeck souligne qu'il existe différentes techniques de *data mining* et que, comme le soulignent les experts juridiques concernés, chaque forme spécifique de *data mining* nécessite d'être abordée séparément et requiert en fait son propre cadre réglementaire.

Il répète donc sa question: s'agit-il d'un seul ou de plusieurs modèles? Et s'il s'agit de plusieurs modèles, sur quelle base déterminera-t-on quel modèle sera appliqué

wordt ingezet op het CAP? Is dat afhankelijk van het aantal zogenaamde *hits* of het aantal *red flags*?

De heer Lode Vereeck vervolgt met de problematiek van modeldrift of modelverval: de verslechtering van de prestaties van dataminingmodellen na verloop van tijd wegens allerlei redenen.

Hij vraagt hoe de minister zal garanderen dat de volledige levenscyclus van dergelijke modellen – ontwerp, validatie, monitoring en desgevallend afbouw – wordt gedocumenteerd. Hoe wordt modelverval opgespoord en hoe wordt bepaald wanneer een model moet worden aangepast of uitgefaseerd?

Hij stipt vervolgens bijkomende vragen aan die afkomstig zijn van Waalse collega's en onderzoekers van de Universiteit van Namen.

Ten eerste vraagt hij hoe gewaarborgd wordt dat modellen met een verhoogd risico op fouten, zoals neurale netwerken, niet worden gebruikt voor gevoelige beslissingen. Dit sluit aan bij zijn eerdere vraag of de administratie één model gebruikt, dan wel verschillende modellen of dataminingtechnieken.

Daarnaast vraagt hij welke voorwaarden de administratie moet vervullen om het eenvoudigste model te gebruiken dat voldoende performant is. Dat is essentieel voor de openbaarheid van bestuur en het recht op een eerlijk proces.

Verder wenst hij te vernemen welke maatregelen worden genomen om te voorkomen dat dataminingmodellen zich voornamelijk richten op relatief gemakkelijk detecteerbare vormen van fraude, terwijl meer complexe en georganiseerde fraudevormen onder de radar blijven.

De heer Vereeck gaat vervolgens in op de bestuurlijke kwaliteit of de openbaarheid van bestuur. Hij merkt op dat de minister meermaals suggereerde dat openbaarheid van bestuur en beroepsmogelijkheden uitsluitend betrekking hebben op de fiscale controlefase, maar dat dit onjuist is: deze beginselen gelden ook voor de selectiebeslissing zelf.

Hij erkent dat het wetsontwerp duidelijk stelt dat automatische risicoclassificatie en dossierselectie slechts suggesties zijn en nooit autonome besluitvorming mogen vormen zonder menselijke toetsing. Dat noemt hij positief. Maar, zo stelt hij, er bestaat geen enkele garantie dat *function creep* dit in de toekomst niet ondermijnt.

au PCC? Le modèle choisi dépendra-il du nombre de réponses positives ou de signaux d'alerte?

M. Lode Vereeck poursuit en abordant la problématique de la dérive des modèles: la détérioration des prestations des modèles de *data mining* au fil du temps pour diverses raisons.

Il demande comment le ministre garantira que le cycle de vie complet de ces modèles – conception, validation, monitoring et, le cas échéant, suppression progressive – sera documenté. Comment détecter la dérive d'un modèle et comment déterminer quand un modèle doit être adapté ou supprimé progressivement?

Il pose ensuite d'autres questions provenant de collègues wallons et de chercheurs de l'université de Namur.

Tout d'abord, il demande comment il sera garanti que les modèles présentant un risque accru d'erreurs, tels que les réseaux neuronaux, ne seront pas utilisés pour prendre des décisions sensibles. Cette question rejoint la précédente, qui visait à savoir si l'administration utilisera un seul modèle ou plusieurs modèles ou techniques de *data mining*.

Il demande également quelles conditions l'administration devra remplir pour utiliser le modèle le plus simple qui soit suffisamment performant. Ce point est essentiel pour la publicité de l'administration et le droit à un procès équitable.

Il souhaiterait également savoir quelles mesures seront prises pour éviter que les modèles de *data mining* ne se concentrent principalement sur les formes de fraude relativement faciles à détecter, sans repérer les formes de fraude plus complexes et organisées.

M. Vereeck aborde ensuite la question de la qualité et de la publicité de l'administration. Il fait observer que le ministre a suggéré à plusieurs reprises que la publicité de l'administration et les possibilités de recours ne concernaient que la phase de contrôle fiscal, mais ce n'est pas exact: ces principes s'appliquent également à la décision de sélection elle-même.

Il reconnaît que le projet de loi prévoit clairement que la classification automatique des risques et la sélection des dossiers ne sont que des suggestions et ne doivent jamais constituer une prise de décision autonome sans contrôle humain. L'intervenant souligne qu'il s'agit là d'un point positif, mais que rien ne garantit qu'un détournement de fonction ne viendra pas compromettre ce principe à l'avenir.

Daarom stelt hij de cruciale vraag: hoe garandeert de minister dat de menselijke tussenkomst van een fiscale ambtenaar een échte en kritische beoordeling inhoudt, en niet louter een formele bekrachtiging van de algoritmische selectie?

Ambtenaren hebben een deontologische plicht maar de spreker heeft daarover toch een aantal concrete vragen. Welke bevoegdheden hebben fiscale ambtenaren om risicoscores te negeren, aan te passen of volledig te verwerpen? Welke procedures bestaan er om ambtenaren te beschermen wanneer zij twijfels hebben over de juistheid of eerlijkheid van een modeluitkomst, zeker aangezien zij de gebruikte parameters niet kennen?

Tegelijkertijd vraagt de spreker hoe wordt voorkomen dat ambtenaren, omgekeerd, blind vertrouwen ontwikkelen in deze risicoscores en daardoor hun beoordelingsvrijheid onbewust beperken. Zit dit element vervat in de opleiding van de ambtenaren?

De heer Vereeck stelde bovendien de vraag in hoeverre interne KPI's, die aan ambtenaren worden opgelegd, de druk zouden kunnen verhogen om de uitkomsten van het model blindelings te volgen.

Tot slot vraagt hij hoe tegenstrijdige conclusies worden behandeld wanneer de menselijke beoordeling niet overeenkomt met de modelsscores. Moet de ambtenaar zich verantwoorden wanneer hij beslist een modelselectie te negeren? Hoe wordt dat behandeld en gedocumenteerd?

De heer Vereeck komt terug op een punt dat de minister zelf eerder aanhaalde: het gebruik van cash of financiële steun van ouders is op zich geen teken van fraude. Daarmee gaat hij akkoord. Maar, zo benadrukt hij, dat sluit niet uit dat dergelijke elementen wél als variabelen in een dataminingmodel kunnen voorkomen.

Hij onderstreept opnieuw dat *money control* niet op zoek gaat naar fraude zelf, maar naar risicogedrag. Precies daarom baart het hem zorgen dat de minister het voorbeeld van cashgebruik en ouderlijke ondersteuning spontaan aanhaalde. De cruciale vraag luidt: hoe garandeert de minister dat een verhoogde risicoscore nooit wordt behandeld alsof die een bewijs van fraude is? Hij vraagt nog expliciet of de minister het ermee eens is dat elke conclusie over fraude moet steunen op feiten en niet op kansberekening.

C'est pourquoi il pose la question cruciale suivante: comment le ministre peut-il garantir que l'intervention humaine d'un agent du fisc consistera en une véritable évaluation critique, et non en une simple validation formelle de la sélection algorithmique?

Les fonctionnaires ont une obligation déontologique, mais l'intervenant se pose tout de même quelques questions concrètes à ce sujet. Quelles sont les compétences dont disposent les agents du fisc pour ignorer, modifier ou rejeter complètement les scores de risque? Quelles sont les procédures existantes pour protéger les agents lorsqu'ils ont des doutes quant à l'exactitude ou la fiabilité d'un résultat de modèle, d'autant plus qu'ils ne connaissent pas les paramètres utilisés?

Parallèlement, l'intervenant demande comment éviter que les fonctionnaires accordent, au contraire, une confiance aveugle à ces scores de risque au point de restreindre inconsciemment leur liberté d'appréciation. La formation des fonctionnaires tient-elle compte de cet élément?

M. Vereeck a également demandé dans quelle mesure les indicateurs clés de performance internes imposés aux fonctionnaires pourraient les presser de suivre aveuglément les résultats du modèle.

Enfin, il demande quel sera le sort réservé aux conclusions contradictoires obtenues en cas de divergence entre l'évaluation humaine et les scores fournis par le modèle. Le fonctionnaire devra-t-il se justifier lorsqu'il décidera d'ignorer une sélection du modèle? Comment ces décisions seront-elles traitées et documentées?

M. Vereeck revient sur un point évoqué précédemment par le ministre lui-même: l'utilisation d'espèces ou l'aide financière accordée par les parents ne constituent pas en soi un signe de fraude. S'il souscrit à cette affirmation, l'intervenant souligne toutefois qu'il n'en demeure pas moins que des éléments de ce type pourront effectivement servir de variables dans un modèle d'exploration des données.

Il souligne à nouveau que *money control* ne recherche pas détecter les fraudes en tant que telles, mais les comportements à risque. C'est justement pourquoi il s'inquiète que le ministre ait spontanément cité les exemples de l'utilisation d'espèces et l'aide financière accordée par les parents. La question cruciale est la suivante: comment le ministre peut-il garantir qu'un score de risque élevé ne sera jamais considéré comme une preuve de fraude? Il demande explicitement si le ministre convient que, pour conclure à une fraude, il faut se fonder sur des faits et pas sur des calculs de probabilité.

Hij stelt verder dat hij nog weinig heeft gehoord over sociaal-wetenschappelijke opleidingen van de ambtenaren hierover. Hij hoopt dat in die opleidingen zeer duidelijk wordt uitgelegd dat een verhoogde kans geen schuld of fout betekent.

Daarnaast vraagt hij hoe de fiscus dit onderscheid ook duidelijk maakt aan burgers. De minister stelde eerder dat in de media “onnodige angst” werd gecreëerd. De heer Vereeck antwoordt dat het dan aan de administratie is om zeer transparant uit te leggen wat het verschil is tussen *money control* en de feitelijke vaststelling van fraude.

De heer Vereeck vervolgt dat hij het tot nu toe uitsluitend heeft gehad over de dossierselectie en niet over de controle zelf. Hij vraagt de minister daarom toe te lichten hoe burgers die onterecht worden aangeduid – bijvoorbeeld door bias, lage datakwaliteit, slechte modellen – snel kunnen worden geholpen om hun naam gezuiverd te krijgen.

Hij wijst erop dat probabilistische modellen onvermijdelijk foutpositieven genereren, en dat dergelijke foutieve aanduidingen gevolgen kunnen hebben voor de betrokken burgers. Daarom stelt hij de vraag: hoe wordt gecontroleerd dat probabilistische signalen niet leiden tot jarenlange registraties of persistente vooroordelen? Met andere woorden: hoe worden burgers beschermd tegen de negatieve en langdurige gevolgen van foutieve risicoscores?

De heer Vereeck richt een aantal vragen over de beveiliging van het dataminingmodel aan de minister.

Hoe zit het met de beveiliging van het dataminingmodel? Welke beveiligingsmechanismen worden toegepast om datalekken te vermijden wanneer de modellen wel op grote datasets worden losgelaten?

Hoe wordt gegarandeerd dat systemen zoals *money control* beschermd zijn tegen *hacking* en externe aanvallen? De spreker verwijst daarbij naar het frequente platleggen van overheidswebsites in de afgelopen maanden en benadrukt de noodzaak van een solide bescherming tegen grootschalige cyberaanvallen, waaronder DDoS-aanvallen.

Hoe wordt gecontroleerd dat back-ups veilig worden bewaard en niet zelf kwetsbaar zijn voor *hacking*?

Il ajoute qu’il n’a guère obtenu d’informations à propos des formations en sciences sociales dispensées aux fonctionnaires à ce sujet. Il espère que ces formations expliqueront très clairement qu’un risque accru n’est pas synonyme de culpabilité ou d’infraction.

Il demande également comment l’administration fiscale expliquera clairement cette distinction aux citoyens. Le ministre a précédemment indiqué que les médias avaient suscité une “peur inutile”. M. Vereeck répond qu’il appartient dans ce cas à l’administration fiscale d’expliquer en toute transparence la différence entre *money control* et la constatation factuelle d’une fraude.

M. Vereeck indique ensuite qu’il n’a évoqué pour l’instant que la question de la sélection des dossiers, et pas celle du contrôle à proprement parler. Il demande donc au ministre d’expliquer comment les citoyens dont le dossier sera sélectionné à tort – en raison, par exemple, d’un biais, d’une mauvaise qualité des données ou de modèles inadéquats – pourront être rapidement aidés à rétablir leur réputation.

Il souligne que les modèles probabilistes génèrent inévitablement des faux positifs et que ceux-ci peuvent avoir des répercussions pour les citoyens concernés. Il demande donc comment on vérifiera que les signaux probabilistes n’entraînent pas d’enregistrements pendant des années ni de préjugés persistants? En d’autres termes, comment les citoyens seront-ils protégés contre les conséquences négatives et durables des scores de risque erronés?

M. Vereeck pose plusieurs questions au ministre à propos de la sécurité du modèle d’exploration de données.

Qu’en est-il de la sécurité du modèle d’exploration de données? Quels mécanismes de sécurité seront mis en œuvre pour éviter les fuites de données lorsque les modèles sont appliqués à de grands ensembles de données?

Comment des systèmes tels que le *money control* seront-ils protégés contre le piratage et les attaques externes? L’intervenant évoque à cet égard les paralysies qui ont fréquemment touché des sites web de pouvoirs publics ces derniers mois, et il souligne la nécessité d’une protection solide contre les cyberattaques à grande échelle, y compris les attaques par déni de service.

Comment sera-t-il vérifié que les sauvegardes seront conservées en toute sécurité et ne seront pas elles-mêmes exposées au piratage?

Welke cybersecuritytests worden uitgevoerd bij de FOD Financiën? En wat waren de resultaten tot nu toe?

De heer Vereeck kondigt aan dat hij, hoewel het al uitgebreid aan bod is gekomen, hij toch kort zal ingaan op de grondrechten. Tot nu toe, zo stelt hij, werd enkel gesproken over formele legaliteit: er moet een wet zijn, en die ligt er nu. Maar dat is slechts het minimale uitgangspunt.

Volgens de juridische analyses waarnaar hij verwijst, vereist formele legaliteit bovendien dat elke datamining-functie duidelijk wordt omschreven en gedefinieerd. Hij stelt dat dit ontbreekt. Ook criteria voor proportionaliteit, zoals: waarom dit model? welk modeltype? welke techniek? ontbreken in de wet. Eveneens ontbreken transparantie- en documentatieplichten en ook *fairness audits*.

Naast de formele legaliteit is er ook de kwalitatieve legaliteit, die inhoudt dat burgers moeten kunnen begrijpen wat de overheid doet en waarom dit mag. Hij betwijfelt of dat het geval is, omdat een burger nooit kan begrijpen waarom een dataminingmodel bepaalde correlaties detecteert. Hij vraagt of de minister erkent dat de kwalitatieve legaliteit hier tekortschiet.

Verder verwijst hij naar de functionele legaliteit, die vereist dat elk type datamining een eigen, specifieke rechtsgrond heeft. Een enkel generiek wetsartikel volstaat volgens de juridisch experts niet.

Dan komt de spreker kort terug op het vermoeden van onschuld. Dat was al bij de bespreking van de beleidsnota in maart zijn eerste grote bekommernis. Hoewel de minister stelt dat het vermoeden van onschuld overeind blijft, is hij zelf daarvan niet overtuigd. Hij stelt dat er zonder enig vermoeden van fraude in rekeningen wordt gekeken. Hij verwijst naar de analyse van Matthias Dobbelaere-Welvaert in het VRT-programma *De Markt*. Die citeerde het arrest nr. 162/2022 van het Grondwettelijk Hof, van 8 december 2022, waarin werd gesteld dat de uitbreiding van het CAP geen inbreuk vormt op de privacy, omdat er voldoende fundamentele waarborgen bestaan, waaronder net het vermoeden van onschuld.

De heer Dobbelaere-Welvaert vraagt zich af waarom de minister ervan uitgaat dat het Grondwettelijk Hof opnieuw eenzelfde oordeel zal vellen, nu dat vermoeden van onschuld volgens hem verdwijnt voordat de cijfers worden ingekeken. In dat arrest was dat vermoeden een

Quels tests de cybersécurité sont effectués au SPF Finances? Et quels en ont été les résultats jusqu'à présent?

M. Vereeck annonce que, bien que cela ait déjà été largement abordé il évoquera brièvement la question des droits fondamentaux. Jusqu'à présent, il indique que seule la légalité formelle a été évoquée: une loi doit être élaborée, et celle-ci est aujourd'hui à l'examen. Mais ce n'est que le minimum.

Selon les analyses juridiques auxquelles il se réfère, la légalité formelle exige en outre que chaque fonction d'exploration des données soit clairement décrite et définie. Il indique toutefois que cette exigence n'est pas remplie. La loi ne définit pas non plus les critères de proportionnalité et ne précise pas pourquoi ce modèle sera utilisé, quel sera le modèle type ni quelle sera la technique utilisée. Il en va de même pour les obligations de transparence et de documentation, ainsi que pour les audits d'équité.

Outre la légalité formelle, il y a la légalité qualitative, qui implique que les citoyens doivent pouvoir comprendre les mesures prises par les pouvoirs publics et la raison pour laquelle ces mesures sont autorisées. L'intervenant doute que ce soit le cas en l'espèce, car un citoyen ne pourra jamais comprendre pourquoi un modèle de *data mining* détecte certaines corrélations. Il demande au ministre s'il reconnaît que la légalité qualitative fait défaut.

Il évoque également la légalité fonctionnelle, qui requiert que chaque type de *data mining* s'appuie sur sa propre base juridique spécifique. Selon les experts juridiques, un seul article de loi générique ne suffit pas.

L'intervenant revient ensuite brièvement sur la présomption d'innocence. C'était déjà sa première préoccupation lors de la discussion de la note de politique générale en mars. Bien que le ministre indique que la présomption d'innocence demeure intacte, l'intervenant n'en est pas convaincu. Il affirme que les comptes seront scrutés sans qu'il y ait présomption de fraude. Il renvoie à l'analyse faite par Matthias Dobbelaere-Welvaert dans l'émission *De Markt* de la VRT. Celui-ci a cité l'arrêt n° 162/2022 rendu le 8 décembre 2022 par la Cour constitutionnelle, qui indique que l'élargissement du PCC ne constitue pas une atteinte au respect de la vie privée, car il existe suffisamment de garanties importantes, dont précisément la présomption d'innocence.

M. Dobbelaere-Welvaert se demande pourquoi le ministre part du principe que la Cour constitutionnelle rendra à nouveau le même verdict, alors que, selon lui, la présomption d'innocence disparaîtra avant même la consultation des chiffres. Dans cet arrêt, cette présomption

essentieel element van de bescherming. Hij stelt dat die bescherming nu terzijde lijkt te worden geschoven.

Over privacy wil hij het niet opnieuw uitgebreid hebben; men verschilt daarover duidelijk van mening. De heer Vereeck is benieuwd hoe de rechtbanken, het Grondwettelijk Hof en eventueel het Europees Hof van Justitie daarover zullen oordelen.

De spreker is wel tevreden dat elke toegang tot het CAP wordt gelogd, zodat *ex post* kan worden nagegaan of er misbruik of ongeoorloofde toegang heeft plaatsgevonden – en dat dit niet alleen geldt voor fiscale ambtenaren, maar ook voor externe partijen, zoals softwareleveranciers, die mogelijk toegang krijgen tot het dataminingmodel.

In dat verband vraagt hij of de minister van plan is een informatiecampagne te ontwikkelen voor burgers over het CAP en het dataminingmodel.

Tot slot gaat de heer Vereeck kort in op proportionaliteit. Ook daarover verschilt men van mening. Het lijkt hem evident dat de screening van miljoenen onschuldige burgers, terwijl slechts een fractie betrokken is bij fiscale fraude, disproportioneel is.

Vervolgens wenst de heer Vereeck het te hebben over dataminimalisatie, een juridische verplichting. Hij wenst te weten hoe het beginsel van minimale gegevensverwerking of dataminimalisatie wordt gerespecteerd wanneer alle financiële gegevens van alle Belgen, jong en oud, automatisch worden bijgehouden en gescreend. Hoe garandeert de minister dat alle verwerkingen strikt voldoen aan het beginsel van dataminimalisatie? Welke mechanismen worden gehanteerd om datamaximalisatie te vermijden?

Een ander aspect betreffende de legale procedures ter bescherming van de fundamentele rechten is het recht op transparantie, het recht op beroep en het recht op een eerlijk proces. Burgers hebben het recht om een beslissing van een overheid aan te vechten. Daarvoor is natuurlijk vereist dat zij weten waarom een overheid een beslissing neemt of genomen heeft. Transparantie en uitlegbaarheid van een beslissing zijn dan ook cruciale rechtsstatelijke waarborgen voor het recht op beroep en een eerlijk proces.

constituait un élément essentiel de la protection. Il indique que cette protection semble désormais être écartée.

M. Vereeck ne souhaite pas revenir en détail sur la question du respect de la vie privée, car les avis divergent clairement à ce sujet. Il est curieux de savoir comment les tribunaux, la Cour constitutionnelle et éventuellement la Cour de justice de l'Union européenne statueront à ce sujet.

L'intervenant se réjouit toutefois qu'il soit prévu que chaque accès au PCC doit être enregistré, ce qui permettra de vérifier *a posteriori* si l'accès a été accordé de façon abusive ou illicite. Il se félicite également que ces enregistrements visent non seulement les fonctionnaires de l'administration fiscale, mais aussi les parties externes, par exemple les fournisseurs de logiciels, qui pourront avoir accès au modèle de *data mining*.

Dans ce contexte, il demande si le ministre a l'intention de mettre en place une campagne d'information à l'intention des citoyens à propos du PCC et du modèle de *data mining*.

Enfin, M. Vereeck évoque brièvement la question de la proportionnalité. Les avis divergent également sur ce point. Il lui semble évident qu'il est disproportionné de contrôler des millions de citoyens innocents, eu égard au nombre restreint de personnes impliquées dans une fraude fiscale.

Ensuite, M. Vereeck souhaite aborder la question de la minimisation des données, qui est une obligation juridique. Il souhaite savoir comment le principe de traitement minimal des données – la minimisation des données – sera respecté si toutes les données financières de tous les Belges, jeunes comme âgés, sont automatiquement conservées et analysées. Comment le ministre garantit-il que tous les traitements répondront strictement au principe de minimisation des données? Quels seront les mécanismes mis en place pour éviter une maximalisation des données?

Le droit à la transparence, le droit de recours et le droit à un procès équitable constituent une autre facette des procédures légales de protection des droits fondamentaux. Les citoyens ont le droit d'attaquer une décision des autorités publiques. À cet effet, ils doivent bien entendu savoir la raison pour laquelle ces autorités publiques prennent ou ont pris une décision donnée. La transparence et la motivation d'une décision sont dès lors des conditions essentielles de l'État de droit pour garantir le droit de recours et le droit à un procès équitable.

Hoewel er een menselijke controle is tijdens de selectie, komt die enkel in de tweede fase aan bod en niet in de eerste fase van de dossierselectie. Hoe kan een burger bezwaar indienen tegen een beslissing als hij niet weet waarom hij geselecteerd is en de ambtenaar dat ook niet kan vertellen? Hoe wordt ervoor gezorgd dat burgers weten hoe ze in beroep kunnen gaan wanneer ze door een geautomatiseerd systeem worden geselecteerd?

Dit brengt de heer Vereeck bij de *counterfactual* of tegenfeitelijke verklaringen. Hoe kunnen rechters, toezichthouders en het Parlement toegang krijgen tot die technische details, zodat effectief toezicht mogelijk is? Zal de minister alsnog een publiek register willen invoeren om aan de vereisten van transparantie te voldoen? Als er geen volledige transparantie wordt geboden aan burgers, aan toezichthouders, aan het Parlement en aan rechters, welke auditmechanismen bestaan er dan eventueel om de informatie- en transparantieplicht alsnog te doen naleven?

Wat de transparantie betreft, wenst de spreker te weten of de geheime selectiecriteria en risicoclusters – zoals ingeschreven in de memorie van toelichting – niet langer geheim mogen blijven vanaf het moment dat ze juridische gevolgen hebben voor burgers. Kan de minister bevestigen dat het geheim rond de selectiecriteria, met name de variabelen die in de fiscale dataminingmodellen zitten en die van strategisch belang zijn, opgeheven wordt zodra de toepassing tot juridische gevolgen leidt voor de burgers? Mogen zij dan die criteria wel kennen?

Tot slot, is de minister bereid om systemen van *counterfactual* verklaringen in te voeren zodat burgers weten welke factoren tot een andere oplossing zouden hebben geleid?

De heer Vereeck benadrukt dat de bestrijding van fraude door iedereen gesteund wordt. Hij meent dan ook dat de wet maar beter robuust kan zijn, maar ziet alvast één belangrijk juridisch probleem, namelijk dat van de transparantie en het recht op een eerlijk proces en het vermoeden van onschuld.

Het gebruik van algoritmes die *counterfactual* of tegenfeitelijke verklaringen geven zou een mogelijke oplossing bieden. Aangezien de minister dit niet heeft besproken, wenst de heer Vereeck hierover nog een aantal vragen te stellen. Zo'n *counterfactual* verklaring zal aangeven welke data veranderd moeten worden opdat de beslissing zou veranderen. Dergelijke verklaringen zijn perfect te begrijpen zonder enige kennis van datamining.

Bien qu'un contrôle humain soit effectué au moment de la sélection, celui-ci n'intervient que lors de la deuxième phase et non lors de la première phase de sélection des dossiers.. Comment un citoyen peut-il introduire une réclamation contre une décision s'il ne sait pas pourquoi il a été sélectionné et si le fonctionnaire n'est pas davantage en mesure de le lui expliquer? Comment s'assurera-t-on que les citoyens sachent comment tenter un recours lorsqu'ils sont sélectionnés par un système automatisé?

M. Vereeck en arrive ainsi aux explications contrefactuelles. Comment les juges, les organes de contrôle et le Parlement pourront-ils avoir accès à ces détails techniques afin d'effectuer un contrôle efficace? Le ministre envisage-t-il d'instaurer un registre public en vue de répondre aux exigences en matière de transparence? À défaut d'une transparence complète vis-à-vis des citoyens, des organes de contrôle, du Parlement et des juges, quels sont les mécanismes d'audit susceptibles d'assurer cette obligation de transparence?

En ce qui concerne la transparence, l'intervenant souhaite savoir si les critères de sélection secrets et les clusters de risques (mentionnés dans l'exposé des motifs) ne doivent pas être révélés à compter du moment où ils entraînent des conséquences juridiques pour les citoyens. Le ministre peut-il confirmer que le secret qui entoure les critères de sélection, qui sont les variables sous-jacentes des modèles de *data mining* fiscal et qui revêtent une importance stratégique, sera levé dès que l'application de ces critères génère des effets juridiques pour les citoyens? Ces derniers pourront-ils alors prendre connaissance de ces critères?

Pour terminer, le ministre est-il prêt à introduire des systèmes d'explications contrefactuelles pour que les citoyens puissent prendre connaissance des facteurs qui auraient conduit à une autre solution?

M. Vereeck souligne que tout le monde soutient la lutte contre la fraude. Il estime dès lors que la législation en la matière se doit d'être solide, mais identifie en tout cas un problème juridique de taille, à savoir celui de la transparence et du droit à un procès équitable et à la présomption d'innocence.

L'utilisation d'algorithmes fournissant des explications contrefactuelles serait une piste envisageable. Puisque le ministre n'a pas abordé la question, M. Vereeck souhaiterait encore poser quelques questions. Ces explications contrefactuelles indiqueront quelles données doivent être modifiées afin de générer une autre décision. Ces explications sont tout à fait compréhensibles, même sans connaissances en *data mining*. Elles doivent cependant

Deze verklaring moet echter persoonsgebonden zijn. De belastingplichtige krijgt dus de transparantie die hij verdient, zonder dat het model of het algoritme zelf openbaar moet worden gemaakt. De belastingplichtige krijgt dus geen informatie over hoe hij de belastingen kan ontwijken, waardoor er ook geen fiscaal verlies is.

Kan de minister bevestigen dat burgers recht hebben op een verklaring die niet enkel uitlegt wat het model heeft gedaan, maar ook waarom het model tot die beslissing is gekomen? Kan de minister ook garanderen dat burgers inzicht krijgen in welke variabelen het sterkst hebben bijgedragen aan hun risicoscore en waarom dit fiscaal relevant is? Is de minister bereid om *counterfactual* verklaringen – die volgens de spreker wel door artificiële intelligentie gegenereerd mogen worden – vrij te geven zodat burgers begrijpen welke factoren tot hun risicoscore hebben geleid? Tot slot, kan de minister garanderen dat burgers toegang krijgen tot zo'n begrijpelijk juridisch relevante tegenfeitelijke uitleg in plaats van louter technische modelbeschrijvingen?

Het lid wenst ook een aantal beleidslessen te trekken uit voorliggend wetsontwerp. De bespreking in de commissie loopt op zijn einde; één spreker heeft 45 uur kunnen spreken. Toch lijkt dit bijzonder weinig voor een belangrijk onderwerp dat niet alleen over fiscaliteit gaat, maar ook over de grondslagen van onze rechtsstaat en het optuigen van een controlestaat. De heer Vereeck wenst te weten of in de toekomst nieuwe beleidsmaatregelen rond fiscale of economische massasurveillance zullen worden onderworpen aan een brede maatschappelijke consultatie, onder andere in het Parlement. Hij roept ook op dergelijke beleidsmaatregelen niet via een amendement te doen bij een omnibuswet, maar daar voldoende tijd voor te nemen.

Daarna verwijst de spreker naar de toeslagenaffaire in Nederland, waarbij het laatste slachtoffer recent vergoed werd. De rechter besliste dat de wetgeving die het mogelijk maakt om geautomatiseerde datamining in te zetten het recht op privacy schendt wegens een gebrek aan transparantie, proportionaliteit en individuele verdenking. Daarbij gaat het niet alleen over de tweede fase, de fiscale controle, maar ook over de eerste fase, met name de dossierselectie. Bijgevolg zou men dus geen geautomatiseerde datamining mogen toepassen, zelfs niet in de eerste fase. Onvoldoende inzicht in de selectiecriteria maakt de inmenging immers disproportioneel. De heer Vereeck wenst dan ook te weten of de minister geen enkele les trekt uit de structurele mislukking van

être liées à la personne. Le contribuable bénéficiera ainsi de la transparence à laquelle il a droit, sans qu'il soit nécessaire de rendre le modèle, voir l'algorithme, public. Aucune information permettant au contribuable de déterminer comment éviter les impôts n'est divulguée et il n'y a donc pas de pertes fiscales.

Le ministre peut-il confirmer que les citoyens ont droit, non pas uniquement à l'explication du fonctionnement du modèle, mais aussi à l'explication de la raison pour laquelle le modèle est arrivé à cette décision? Le ministre peut-il également garantir que les citoyens pourront prendre connaissance des variables ayant le plus pesé dans leur score de risque et de la raison pour laquelle elles sont pertinentes du point de vue de l'analyse fiscale? Le ministre est-il disposé à communiquer des explications contrefactuelles (qui, aux yeux de l'intervenant, peuvent être générées par intelligence artificielle) pour permettre aux citoyens de comprendre quels facteurs ont déterminé leur score de risque? Enfin, le ministre peut-il garantir que les citoyens auront accès à des explications contrefactuelles pertinentes et formulées dans un langage juridique clair plutôt qu'à des descriptions de modèle purement techniques?

Le membre souhaite également tirer une série de leçons politiques du projet de loi à l'examen. La discussion en commission touche à sa fin et un seul intervenant est parvenu à parler pendant 45 heures. Pour autant, cela semble relativement peu pour un sujet d'une telle importance, qui ne touche pas uniquement à la fiscalité, mais aussi aux fondements de notre État de droit, et révèle l'émergence d'un État de contrôle. M. Vereeck souhaite savoir si, à l'avenir, les prochaines mesures politiques relatives à une surveillance de masse en matière fiscale et économique seront soumises à une large consultation publique, notamment au parlement. Il en appelle également à ne pas proposer de telles mesures politiques sous la forme d'un amendement à une loi omnibus, mais plutôt à y consacrer suffisamment de temps.

L'intervenant évoque ensuite l'affaire des allocations aux Pays-Bas, dans laquelle la dernière victime a été indemnisée récemment. Le juge a estimé que la législation qui permettait le *data mining* automatisé enfreignait la protection de la vie privée en raison d'un manque de transparence, de proportionnalité et de suspicion individuelle. La deuxième phase, à savoir le contrôle fiscal, n'est pas la seule concernée; la première phase, à savoir la sélection des dossiers, l'est également. Par conséquent, le *data mining* automatisé ne devrait pas être autorisé, même lors de la première phase. En effet, en raison d'une transparence insuffisante des critères de sélection, l'ingérence est à considérer comme disproportionnée. M. Vereeck souhaite dès lors savoir si

datagedreven massasurveillances, voor de ontwikkeling van *money control*.

In zijn slotbedenkingen vraagt de heer Vereeck of het sop wel de kool waard is. Zelf wil hij niet dat zijn kinderen opgroeien in een controlemaatschappij. Waarom neemt de minister dit initiatief? Wegen de baten van *money control* op tegen de kosten ervan, en wat zijn de baten of de voordelen ervan? Er spelen ongetwijfeld puur politieke motieven en budgettaire redenen mee.

De heer Vereeck heeft getracht een soort van kosten-batenanalyse te maken om te zien waarom de minister doorgaat met dit wetsontwerp. Uit de beleidsnota en de notificatie van het budgettaire traject van 2025 tot 2029 leidt hij af dat *money control* 600 miljoen euro moet opbrengen. Dat is namelijk het bedrag dat wordt ingeschreven in 2029. Dat wordt afgezonderd van de sociale fraude, die ook nog eens 600 miljoen euro moet opbrengen, en de e-facturatie waardoor het moeilijker zal zijn om te frauderen met btw-facturen.

Wat de kosten betreft, somt de spreker eerst de nadelen van het project op: de ondermijning van de rechtsstaat omdat er geen minimumvereisten zijn voor de legaliteit; geen vermoeden van onschuld; inbreuken op de privacy; geen proportionaliteit; geen dataminimalisatie; geen recht op een eerlijk proces in beroep; niet langer schuld of fraude, maar statistische schuld of risico; indirecte discriminatie door bias; de valspositieven, die erger zijn dan valsnegatieven, want ze veroordelen onschuldige burgers; de *function creep* nu en in de toekomst; de doelbinding wordt doorgeknipt en er is geen enkele garantie dat dat in de toekomst ook niet gebeurt; de *chilling effects* die uiteindelijk zullen leiden tot minder innovatie.

Daaruit concludeert de heer Vereeck dat de regering voor 600 miljoen euro alle rechtsstatelijke principes in de vuilbak gooit en dat de kosten niet opwegen tegen de baten. Bestaan er geen alternatieven die eenzelfde bedrag als *money control* kunnen opbrengen zonder al de opgesomde nadelen? Wat waren de alternatieven en werden ze überhaupt overwogen? Volgens de spreker zijn preventie van fraude, sensibiliseringscampagnes, gerichte nudging en vooral fiscale vereenvoudiging mogelijke alternatieven. Er kan maar fraude ontstaan als de fiscaliteit dermate complex is dat ze omzeild kan worden, en het bijna niet te detecteren valt. Dus

le ministre n'a vraiment tiré aucune leçon de l'échec structurel des surveillances de masse s'appuyant sur un traitement des données au moment d'élaborer la législation *money control*.

Dans ses conclusions, M. Vereeck se demande si le jeu en vaut la chandelle. En ce qui le concerne, il ne souhaite pas que ses enfants grandissent dans une société de la surveillance. Pourquoi le ministre prend-il cette initiative? La plus-value de la législation *money control* contrebalance-t-elle les coûts qu'elle génère? Et quels sont les bénéfices ou les avantages de cette politique? Des motifs purement politiques et budgétaires entrent indéniablement en ligne de compte.

M. Vereeck s'est essayé à un genre d'analyse coûts-bénéfices afin de comprendre pourquoi le ministre maintenait ce projet de loi. Il déduit de la note de politique générale et du trajet budgétaire de 2025 à 2029 que la législation *money control* rapportera 600 millions d'euros. C'est en tout cas le montant inscrit en 2029. Ce montant est à dissocier de la lutte contre la fraude sociale, qui doit également rapporter 600 millions d'euros, et de la facturation électronique, qui compliquera la fraude à la TVA.

S'agissant des coûts, l'intervenant énumère d'abord les inconvénients du projet: atteinte à l'état de droit dès lors qu'aucune exigence minimale n'est prévue concernant la légalité, aucune présomption d'innocence, violations de la vie privée, aucune proportionnalité, aucune minimisation des données, aucun droit de recours équitable, remplacement de la culpabilité ou de la fraude par une culpabilité statistique ou un risque de fraude, discriminations indirectes dues à des biais, faux positifs (qui sont encore plus graves que les faux négatifs dès lors qu'ils débouchent sur la condamnation de citoyens innocents), détournement de la finalité aujourd'hui et à l'avenir, réduction de la limitation des finalités et aucune garantie que cela ne se répétera pas à l'avenir, effet paralysant (*chilling effects*) qui débouchera sur une baisse de l'innovation.

M. Vereeck conclut de ce qui précède que le gouvernement sacrifie tous les principes de l'état de droit pour 600 millions d'euros, et que les bénéfices du dispositif ne l'emportent pas sur ses coûts. N'existerait-il pas de mesures alternatives susceptibles de rapporter autant que *money control* sans toutefois présenter tous les inconvénients énumérés? Quelles étaient les solutions alternatives, et celles-ci ont-elles réellement été envisagées? Selon l'intervenant, la prévention de la fraude, les campagnes de sensibilisation, l'incitation comportementale (*nudging*) ciblée et, surtout, la simplification fiscale sont des pistes alternatives possibles. La fraude

waarom zet de regering niet fundamentele in op fiscale vereenvoudiging?

Waarom wordt er niet meer geïnvesteerd in traditionele, heel gerichte fiscale opsporing in plaats van in deze generieke massasurveillance? Is er ook al gekeken naar andere fiscale fraude, zoals btw-fraude die meer zou kunnen opbrengen? De spreker verwijst ter illustratie naar een rapport van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) in Nederland over het gebruik van fiscale datamining, dat begint met een overzicht van fraude in alle verschillende domeinen van de fiscaliteit. Had men deze oefening ook in België gedaan, dan had men misschien beslist eerder voor een andere aanpak te kiezen. Is de regering bereid om in plaats van een populatiebrede screening met bias door te voeren, eerder een *random sampling* te doen?

Indien de regering toch doorgaat met dit project, dan wenst de heer Vereeck een aantal remedies voor te stellen: verplichte tegenfeitelijke verklaringen, de oprichting van een onafhankelijke toezichthouder die een audit en analyse van data en algoritmes doet, meer procedurele en wettelijke waarborgen in dit wetsontwerp rond doelbinding, recht op inzage en beroep, rechtsherstel enzovoort. Ook een impactanalyse ontbreekt. Daarnaast zijn investeringen in vertrouwen, communicatie, transparantie, proportionele sancties en respect nodig om het *chilling effect* dat het sociaal kapitaal van de samenleving vernietigt een beetje te herstellen. Tot slot is er nood aan een verscherpte parlementaire controle.

De heer Hugues Bayet (PS) bedankt de minister voor zijn antwoorden, maar licht toe dat zijn fractie om verschillende redenen tegen het geheel van artikelen van dit wetsontwerp houdende diverse bepalingen zal stemmen.

De eerste reden betreft de flexi-jobs. De minister geeft aan dat flexi-jobs in bepaalde sectoren noodzakelijk zijn. Zelfs als socialist is de spreker het daarmee eens, maar hij vraagt waarom de minister de flexi-jobs naar alle sectoren wil uitbreiden. De minister verhoogt de grens alleen maar van 12.000 naar 18.000 euro omdat hij niet in staat is een fiscale hervorming door te voeren. Zo stelt de minister de burgers in de mogelijkheid meer te werken om meer te verdienen, aangezien hij er niet voor kan zorgen dat ze per maand 500 euro netto extra zullen verdienen. Zulks zal de concurrentie tussen de werknemers doen toenemen. Bovendien trekt

ne peut exister que si la fiscalité est tellement complexe qu'elle peut être contournée et que si elle est presque impossible à détecter. Dès lors, pourquoi le gouvernement ne mise-t-il pas davantage sur la simplification fiscale?

Pourquoi n'investit-il pas davantage dans la recherche classique et très ciblée de la fraude fiscale plutôt que d'instaurer cette surveillance de masse générique? S'est-on déjà aussi intéressé à la lutte contre d'autres formes de fraude fiscale, comme la fraude à la TVA, qui pourraient rapporter davantage? En guise d'exemple, l'intervenant renvoie à un rapport du Conseil scientifique néerlandais pour la politique gouvernementale (*Wetenschappelijke Raad voor het Regeringsbeleid* (WRR)) sur l'utilisation de l'exploration de données à des fins fiscales, qui s'ouvre sur un aperçu de la fraude dans les différents domaines de la fiscalité. Si cet exercice avait aussi été réalisé en Belgique, on aurait peut-être décidé d'opter plutôt pour une autre approche. Le gouvernement serait-il prêt à procéder à un échantillonnage aléatoire plutôt que de réaliser un *screening* biaisé à l'échelle de la population?

Si le gouvernement poursuit tout de même la mise en œuvre de ce projet, M. Vereeck souhaiterait proposer un certain nombre de mesures correctives: explications contrefactuelles obligatoires, création d'un organisme de contrôle indépendant chargé d'auditer et d'analyser les données et les algorithmes, renforcement des garanties procédurales et légales dans le texte à l'examen concernant la limitation des finalités, droit de consultation et de recours, réparation, etc. Une analyse d'impact fait également défaut. En outre, des investissements dans la confiance, de la communication, de la transparence, des sanctions proportionnées et du respect seront nécessaires pour contrecarrer quelque peu l'effet paralysant qui détruira le capital social de la société. Enfin, un contrôle parlementaire accru sera nécessaire.

M. Hugues Bayet (PS) remercie le ministre pour ses réponses, mais explique que son groupe votera contre l'ensemble des articles de ce projet de loi portant des dispositions diverses, et cela pour plusieurs raisons.

La première raison concerne les flexi-jobs. Le ministre indique que les flexi-jobs sont nécessaires dans certains secteurs. Même en tant que socialiste, l'intervenant est d'accord, mais il se demande pourquoi le ministre veut étendre les flexi-jobs à tous les secteurs. Le ministre augmente la limite de 12.000 à 18.000 euros uniquement parce qu'il n'est pas capable de réaliser une réforme fiscale. Ainsi, le ministre permet aux citoyens de travailler plus pour gagner plus, vu qu'il lui est impossible de garantir qu'ils gagneront 500 euros nets en plus par mois. Cela va accroître la concurrence entre les travailleurs. En outre, le ministre définance la sécurité sociale, avec

de minister middelen weg uit de sociale zekerheid, met een inkomstenderving ten belope van 480 miljoen euro, wat voor de spreker en zijn fractie onaanvaardbaar is.

Inzake de onderhoudsuitkeringen en de zogenoemde “echtscheidingstaks” is de heer Bayet van oordeel dat de minister geen antwoord geeft op zijn bezorgdheid betreffende de verarming van de rechthebbenden, voornamelijk alleenstaande moeders die dergelijke onderhoudsuitkeringen ontvangen om hun kinderen groot te brengen. Een en ander zou de staat ongeveer 20 miljoen euro moeten opleveren. Het is echter niet duidelijk welk bedrag zal worden geheven. De spreker raamt dat het 30 tot 40 euro per maand zal zijn. Kan de minister dat bevestigen?

Inzake de Dienst voor alimentatievorderingen (DAVO) geeft de minister aan dat hij weldra een wetsontwerp zal voorleggen. Zou hij het Parlement al iets kunnen vertellen over wat daarin zal staan? Zullen de voorschotten worden opgetrokken? Zal het wetsontwerp rekening houden met de door alle partijen in het Parlement aangenomen resolutie die ertoe strekt de inlichtingen inzake de toegang tot de DAVO te verbeteren? Wat zijn de voorgenomen termijnen in dat verband?

De heer Bayet gaat in op wat de minister “fiscale niches” noemt, maar wat de spreker veeleer kleingeestige maatregelen vindt. De verwachte opbrengst daarvan is toch echt heel gering. De minister richt zijn pijlen met name op de uitgaven in het raam van een adoptieprocedure en op de vrijgevigheid van de Belgen. Voorts blijft deze regering herhalen dat ze werk en werknemers beoogt te beschermen, maar de maatregel voor verre verplaatsingen wordt wel opgeheven. Werknemers die meer dan 75 kilometer afleggen om naar hun werk te gaan, moeten voortaan niet meer op dat bijkomend forfait rekenen.

Wat de aanslag- en onderzoekstermijnen van het Wetboek van de inkomstenbelastingen 1992 betreft, is de minister van oordeel dat fraudebestrijding niet gebaat zou zijn bij langere termijnen. De spreker ziet dat anders: het kan toch geen slechte zaak zijn dat de FOD meer tijd heeft om onderzoek te doen? Bovendien werd na afloop van de bijzondere commissie “internationale fiscale fraude/Panama Papers” (DOC 54 2749/001) onder meer de aanbeveling gedaan bepaalde termijnen te verlengen.

De spreker feliciteert de minister met de amendementen betreffende de werking van het Centraal Aanspreekpunt van rekeningen en financiële contacten (CAP). Die zullen de fraudebestrijding aanzienlijk verbeteren. Precies

480 millions d’euros de manque à gagner, ce qui est inacceptable pour l’intervenant et son groupe.

En ce qui concerne les rentes alimentaires et la soi-disant “taxation sur le divorce”, M. Bayet estime que le ministre ne répond pas à ses craintes d’appauvrissement des bénéficiaires, principalement des mères seules qui perçoivent ces pensions pour élever leurs enfants. Cela devrait rapporter environ 20 millions d’euros à l’État. Il n’est pas clair quel montant sera prélevé. L’intervenant estime qu’il s’agira de 30 à 40 euros par mois. Le ministre peut-il confirmer cela?

Pour ce qui est du Service des créances alimentaires (SECAL), le ministre indique qu’il soumettra prochainement un projet de loi. Pourrait-il déjà informer le Parlement de ce que contiendra ce projet de loi. Y aura-t-il une augmentation des avances? Le projet de loi tiendra-t-il compte de la résolution votée par le Parlement tous partis confondus qui vise à améliorer l’information à l’accessibilité au SECAL? Quels sont les délais prévus?

M. Bayet revient sur ce que le ministre appelle les “niches fiscales”, mais qu’il considère lui-même comme des mesures mesquines. Les rendements prévus sont vraiment très bas. Le ministre s’attaque notamment aux frais d’adoption et à la générosité des Belges. De plus, ce gouvernement ne cesse de répéter qu’il protège le travail et les travailleurs, mais il supprime la mesure sur les déplacements longs. Les travailleurs qui font plus de 75 kilomètres pour se rendre à leur travail ne pourront désormais plus bénéficier de cette ristourne.

Concernant les délais d’imposition d’investigation du code d’impôt sur les revenus des TVA, le ministre estime que l’allongement des délais en cas de fraude ne permettrait pas d’améliorer la lutte contre la fraude fiscale. D’après l’intervenant, cela laisserait tout de même plus de temps au SPF pour investiguer, ce qui ne peut être négatif. L’allongement des délais faisait par ailleurs partie des recommandations de la commission spéciale “Fraude fiscale internationale/Panama Papers” (DOC 54 2749/001).

L’intervenant félicite le ministre pour les amendements sur le fonctionnement du Point de contact central des comptes et contrats financiers (PCC) qui vont vraiment améliorer la lutte contre la fraude, mais il se demande

daarom vraagt de spreker waarom de minister terugkomt op een maatregel die voorziet in meer tijd om fraudeurs op te sporen.

De heer Dieter Van Besien (Ecolo-Groen) dankt de minister voor zijn uitgebreide, volledige en duidelijke antwoorden, vooral rond de datamining van het CAP. De minister heeft een passioneel en overtuigend pleidooi gehouden voor de datamining van het CAP in het kader van de strijd tegen fiscale fraude. Ook de spreker is hiervan overtuigd en zal dit stuk van de diverse bepalings steunen.

Wat het pleidooi van collega Verkeyn in verband met de flexi-jobs betreft, is de spreker minder overtuigd. Die aanpassingen zal hij dan ook niet steunen. Wat mevrouw Verkeyn vandaag gezegd heeft, lijkt in lijn te zijn met het antwoord van de minister, maar het is wel iets anders dan wat ze tijdens een vorige commissievergadering gezegd heeft. De heer Van Besien is het echter nog steeds niet eens met deze visie.

De heer Vincent Van Quickenborne (Open Vld) dankt de minister om de parlementsleden inzage te geven in de vertrouwelijke DAM-fiche, die in het Frans opgesteld is.

Tijdens de tussenkomsten van de collega's kwamen verschillende landen en hun systemen voor fraudebestrijding aan bod. Zelf heeft de heer Van Quickenborne de systemen in de 27 Europese lidstaten bestudeerd, waarbij hij tot verschillende conclusies kwam. Zo hebben Malta en Cyprus zich geïnspireerd op Luxemburg. Het model van Hongarije en Polen kan hij absoluut niet verdedigen en heeft hij in zijn betoog achterwege gelaten. Toch merkt hij op dat collega Verkeyn het Poolse systeem heeft vermeld, dat heel ver gaat doordat het niet alleen een CAP heeft maar er ook wordt gedatamined op bepaalde gegevens in die CAP. Is dit model, ontwikkeld door de extremistische Poolse PiS-partij, dan het model voor de N-VA?

Mevrouw Charlotte Verkeyn (N-VA) repliceert dat ze niets gezegd heeft over dat CAP-model, maar dat ze verwezen heeft naar een arrest van het Hof van Justitie van de Europese Unie tegen Polen in verband met staatssteun.

De heer Vincent Van Quickenborne (Open Vld) herhaalt dat het Poolse model volgens hem als voorbeeld gediend heeft voor wat de minister nu voorstelt voor België. Zelf meent hij dat dit niet de juiste weg is.

pourquoi le ministre revient sur une mesure qui devrait laisser plus de temps pour traquer les fraudeurs.

M. Dieter Van Besien (Ecolo-Groen) remercie le ministre pour ses réponses détaillées, exhaustives et claires, surtout en ce qui concerne l'extension du PCC au *data mining*. Le ministre a tenu un plaidoyer passionné et convaincant en faveur de cette extension dans le cadre de la lutte contre la fraude fiscale. L'intervenant est lui aussi convaincu par cette mesure, et il soutiendra donc ce volet des dispositions diverses.

L'intervenant est en revanche moins convaincu par le plaidoyer de sa collègue Verkeyn concernant les flexi-jobs. Il ne soutiendra donc pas les modifications proposées en la matière. Les propos tenus aujourd'hui par Mme Verkeyn semblent s'inscrire dans le droit fil de la réponse du ministre, mais ils diffèrent toutefois de ceux qu'elle avait tenus au cours d'une précédente réunion de commission. M. Van Besien rejette cependant toujours cette position.

M. Vincent Van Quickenborne (Open Vld) remercie le ministre d'avoir permis aux députés de consulter la fiche DAM confidentielle, établie en français.

Durant les interventions de ses collègues, plusieurs pays et leurs systèmes respectifs de lutte contre la fraude ont été évoqués. M. Van Quickenborne a lui-même étudié les systèmes en vigueur dans les 27 États membres de l'Union européenne, ce qui lui a permis de tirer plusieurs conclusions. Il a par exemple constaté que Malte et Chypre se sont inspirées du Luxembourg. Il ne peut par ailleurs absolument pas défendre le modèle de la Hongrie et de la Pologne, qu'il a omis d'évoquer lors de son intervention. Il fait cependant observer que sa collègue Verkeyn a mentionné le modèle polonais, dont les implications sont étendues puisqu'il prévoit non seulement un PCC, mais aussi le traitement de certaines informations qui y sont contenues à des fins de *data mining*. Faut-il en déduire que ce modèle, élaboré par le parti polonais extrême PiS, est le modèle à suivre selon la N-VA?

Mme Charlotte Verkeyn (N-VA) rétorque qu'elle n'a rien dit à propos de ce modèle de PCC, mais qu'elle a renvoyé à un arrêt de la Cour de justice de l'Union européenne rendu contre la Pologne en matière d'aides d'État.

M. Vincent Van Quickenborne (Open Vld) réitère qu'à ses yeux, le modèle polonais a servi d'exemple à ce que le ministre propose aujourd'hui pour la Belgique. Il considère à titre personnel qu'il ne s'agit pas de la bonne voie à suivre.

Het feit dat de minister zo uitgebreid geantwoord heeft op de vragen van de parlementsleden wijst er volgens het lid op dat de zeven alinea's van amendement nr. 16 van de regering (DOC 56 0963/005, p. 11-13) veel meer uitleg verdienden. Tot een week geleden bestond er geen enkel debat over het thema; sindsdien wijdden fiscale experts en leken er heel veel aandacht aan in televisieprogramma's, verslagen, artikels. Er is veel interesse voor het ontwerp van de minister en zelfs burgers hebben er plots een mening over. Ook de opname van de commissievergadering werd gretig bekeken, wat een goede reclame is voor het parlementaire werk en dus voor de democratie.

De heer Van Quickenborne verwijst onder meer naar de *Tax TV Show* van fiscalist Jan Tuerlinckx op LinkedIn. Daarin bevestigen een aantal grote fiscale experts dat er hier wel degelijk sprake is van *money control*. Ook wetenschapper Lieven Scheire zegt absoluut voor sociale of fiscale fraudebestrijding te zijn, maar vindt dat *money control* te ver gaat.

Ondanks de uitgebreide antwoorden van de minister is de heer Van Quickenborne van oordeel dat die antwoorden niet volstaan want de bedoeling van de meerderheid is de oppositie het zwijgen op te leggen. Maar de minister kan de Belgen die een bank- of spaarrekening hebben geenszins het zwijgen opleggen. En bij hen is er totaal geen draagvlak voor wat de minister voorstelt. Tijdens de voorbije uitzending van het televisieprogramma *De Tafel van Tine* werd de kijkers de vraag gesteld wat ze van *money control* vinden. Uit de stemming bleek dat 79 % van de kijkers tegen *money control* was, ook al was op dat ogenblik het debat erover nog niet volledig losgebarsten.

Hij wijst er ook op dat collega Michel reeds in mei 2025 als eerste hiervoor heeft gewaarschuwd, toen hij de minister een vraag stelde over *money control*.

De heer Lode Vereeck (VB) komt tussen om erop te wijzen dat hij reeds in maart 2025, tijdens de bespreking van de beleidsverklaring, is tussengekomen over wat nu *money control* genoemd wordt.

De heer Mathieu Michel (MR) voegt eraan toe dat hij tijdens de vorige regering bezwaar maakte tegen *money control* en er nog steeds hetzelfde over denkt.

De heer Niels Tas (Vooruit) benadrukt dat er altijd een menselijke tussenkomst zal zijn. De opsporing van fiscale fraude wordt dus niet volledig overgelaten

L'intervenant estime que le fait que le ministre ait apporté des réponses aussi détaillées aux questions des députés indique que les sept alinéas de l'amendement n° 16 du gouvernement (DOC 56 0963/005, p. 11-13) méritaient bien plus d'explications. Jusqu'il y a une semaine, ce sujet ne faisait pas l'objet du moindre débat, mais, depuis lors, des experts fiscaux et des non-initiés y ont consacré énormément d'attention dans des programmes télévisés, des rapports et des articles. Le projet du ministre suscite beaucoup d'intérêt, et même les citoyens ont soudainement un avis sur la question. L'enregistrement de la réunion de commission a aussi été largement visionné, ce qui constitue une bonne publicité pour le travail parlementaire et, partant, pour la démocratie.

M. Van Quickenborne renvoie notamment à l'émission *Tax TV Show* du fiscaliste Jan Tuerlinckx sur LinkedIn, dans laquelle plusieurs experts fiscaux de renom ont confirmé que le projet de loi à l'examen serait effectivement synonyme de *money control*. Le scientifique Lieven Scheire a quant à lui déclaré être totalement favorable à la lutte contre la fraude sociale et fiscale, tout en estimant que le projet de *money control* va trop loin.

M. Van Quickenborne estime que, bien que détaillées, les réponses du ministre sont insuffisantes, car l'objectif de la majorité est de museler l'opposition. Mais le ministre ne pourra pas museler tous les Belges qui ont un compte bancaire ou un compte d'épargne! Et ceux-ci ne soutiennent absolument pas le projet du ministre. Au cours de la dernière émission du programme télévisé flamand *De Tafel van Tine*, les téléspectateurs ont été invités à donner leur avis sur le projet de *money control*. Selon le sondage réalisé, 79 % d'entre eux y étaient opposés, alors que le débat à ce sujet n'avait alors pas encore atteint son paroxysme.

Le membre souligne également que son collègue Michel a été le premier, dès mai 2025, à lancer une mise en garde en la matière, lorsqu'il a posé une question au ministre à propos du *money control*.

M. Lode Vereeck (VB) fait observer que, dès mars 2025, durant la discussion de l'exposé d'orientation politique du ministre, il était intervenu à propos de ce que l'on appelle aujourd'hui le *money control*.

M. Mathieu Michel (MR) ajoute qu'il avait formulé des objections contre le *money control* sous le gouvernement précédent, et qu'il n'a pas changé d'avis depuis lors.

M. Niels Tas (Vooruit) souligne qu'une intervention humaine sera toujours prévue. La détection de la fraude fiscale ne sera donc pas totalement laissée à

aan algoritmes en AI, zoals de heer Van Quickenborne verkeerdelijk doet uitschijnen.

De heer Vincent Van Quickenborne (Open Vld) repleert dat de liberale partijen in de vorige regering het dataminingproject hebben tegengehouden omdat ze vinden dat het disproportioneel en veel te intrusief is. Op het recente ITAA-congres heeft de heer Bouchez duidelijk gemaakt dat hij nog steeds tegen het project is, maar dat hij niet anders kon dan het vandaag goed te keuren. De eerste minister legt dit ontwerp op ondanks weerstand in zijn eigen regering en het feit dat er absoluut geen draagvlak voor bestaat.

Toen de spreker aandacht vroeg voor het thema, had hij twee doelen voor ogen. Zijn eerste doel was interesse wekken voor het CAP en *money control* bij zijn collega-parlementsleden. Dat lijkt alvast deels gelukt, aangezien velen eindelijk weten dat er een CAP bestaat en welke informatie het bevat en wat de overheid dus reeds over elk van ons weet. Dankzij de lezing van het commissieverslag tijdens de plenaire zitting hoopt de heer Van Quickenborne nog meer collega's te informeren.

Zijn tweede doel was het thema op de politieke agenda te plaatsen, want het werk van parlementen krijgt niet altijd de aandacht die het verdient, ondanks de vele vragen die parlementen van zowel meerderheid als oppositie hierover stellen. Dit onderwerp heeft intussen echter veel aandacht gekregen.

De heer Van Quickenborne dankt dan ook alle personen die hem gesteund hebben om zo veel aandacht te besteden aan dit onderwerp. Het feit dat het Parlement deze strijd voert is immers het beste bewijs dat de democratie levend is, want democratie is veel meer dan politiek en het Parlement. Democratie is de mensen laten spreken, de mensen in alle vrijheid hun gedachten laten zeggen, wat ze de voorbije dagen massaal gedaan hebben. De spreker benadrukt ook dat liberalen pro technologie en pro vooruitgang zijn, en ook pro innovatie en pro vrijheid. Maar het is niet omdat iets technologisch kan dat het ook mag, zeker als het gaat over de overheid.

De heer Van Quickenborne vervolgt dat zijn partij voorstander is van de vooruitgang en van de vrijheid. Maar het is niet omdat iets technologisch mogelijk is, dat het ook moet worden toegelaten. En dat geldt in het bijzonder voor de overheid. In dat geval huldigt de spreker het gezegde "*watch your back*". Hij heeft meer vertrouwen in een kleine overheid die zich beperkt tot

des algorithmes et à l'intelligence artificielle, comme M. Van Quickenborne le laisse accroître.

M. Vincent Van Quickenborne (Open Vld) rétorque que, sous le gouvernement précédent, les partis libéraux se sont opposés au projet de *data mining* parce qu'ils le jugeaient disproportionné et beaucoup trop intrusif. Au cours du récent congrès de l'ITAA, M. Bouchez a indiqué clairement qu'il était toujours opposé à ce projet, mais qu'il n'avait aujourd'hui pas d'autre choix que de l'approuver. Le premier ministre impose ce projet malgré l'opposition qu'il soulève dans ses propres rangs et le fait qu'il ne suscite absolument pas l'adhésion.

Lorsque l'intervenant a demandé que l'on s'intéresse à ce sujet, il poursuivait deux objectifs. Le premier était que ses collègues parlementaires s'intéressent au PCC et au *money control*. Il semble en tout cas y être parvenu en partie, étant donné que nombre d'entre eux savent aujourd'hui enfin qu'un PCC existe, quelles informations y sont contenues et ce que l'administration sait donc déjà sur chacun de nous. En donnant lecture du rapport de commission en séance plénière, M. Van Quickenborne espère informer encore davantage de collègues à ce sujet.

Son second objectif était d'inscrire ce sujet à l'ordre du jour politique, car le travail des parlementaires ne bénéficie pas toujours de l'attention qu'il mérite, malgré les nombreuses questions que les parlementaires de la majorité et de l'opposition posent à ce sujet. Depuis lors, ce sujet a toutefois bénéficié d'énormément d'attention.

M. Van Quickenborne remercie donc toutes les personnes qui l'ont soutenu dans sa volonté de donner le maximum d'exposition à ce sujet. Le fait que le Parlement mène ce combat est en effet la meilleure preuve de la vivacité de notre démocratie, car la démocratie va bien au-delà de la politique et du Parlement. La démocratie, c'est en effet permettre aux citoyens de s'exprimer, d'exprimer leur opinion en toute liberté, ce qu'ils ont fait massivement ces derniers jours. L'intervenant souligne aussi que les libéraux sont favorables à la technologie et au progrès, mais aussi à l'innovation et à la liberté. Mais ce n'est pas parce que quelque chose est technologiquement faisable qu'il faut l'autoriser, *a fortiori* lorsque cela concerne l'administration.

M. Van Quickenborne poursuit en indiquant que son parti défend le progrès et la liberté, mais ce n'est pas parce qu'une chose est possible sur le plan technologique qu'elle doit être autorisée. Et cela vaut en particulier pour les pouvoirs publics. En l'occurrence, l'intervenant recommande de suivre l'adage "*watch your back*" ("sois sur tes gardes"). Il a davantage confiance en une petite

haar kerntaken, dan in een overheid die alles naar zich toetrekt en massaal gegevens van burgers exploiteert.

Het meest gehoorde argument inzake *money control* is dat de overgrote meerderheid van de burgers toch niets te verbergen heeft; ze zijn geen fraudeurs: ze werken, ondernemen en sparen. Maar hoe ver mag de overheid daarin gaan? Wat ze nu voorstelt staat gelijk met het hangen van een camera boven elke bankrekening van alle Belgen en alle ondernemingen.

De spreker vervolgt met het bevestigen dat elke vorm van fraude te veroordelen is. Maar daarover gaat het hier niet. Het gaat erover dat alle bankrekeningen van alle Belgen in het systeem worden gestopt met het oog op dossierselectie. Dat is een enorme hoeveelheid data. Zo zou het gaan over 55 miljoen actieve bankrekeningen in het CAP. Daaraan moeten worden toegevoegd alle saldi, alle bankrekeningen van ondernemingen en alle financiële contracten. Het gaat dan om een half miljard aan data. Echter, die data behoren tot de privésfeer van de burgers en werden nooit vrijwillig gedeeld met de fiscus. Tot nu kon die informatie over bankrekeningen enkel worden geraadpleegd bij aanwijzingen van belastingontduiking (artikel 322 WIB). Die toestand wordt nu fundamenteel omgekeerd want alle financiële gegevens worden nu zonder onderscheid in de systemen van de FOD Financiën gestopt.

Volgens de spreker verdedigt de minister zich met de bewering dat datamining reeds lang bestaat. Maar dat gold tot nu alleen voor gegevens die burgers verplicht moesten delen met de fiscus, bijvoorbeeld in het kader van de belastingaangifte. Nu gebruikt de fiscus echter privégegevens die de burgers niet zelf delen. De heer Van Quickenborne spreekt over “money control”. Er zullen zelfs 377 extra fiscale controleurs worden aangeworven om extra controles uit te voeren en alle data van de burgers te exploiteren. Duizenden “bomma’s” en “bompa’s” zullen zich zorgen moeten maken op het einde van het jaar. Het wordt een fiscale heksenjacht op alle Belgen. De maatregel wordt volgens de spreker ingevoerd op vraag van de regeringspartij Vooruit omdat er zo geen vermogenskadaster moet worden aangelegd. Er wordt wel gemikt op het openstellen van het CAP omdat zich daar alle financiële informatie van alle Belgen bevindt. Zo wordt de deur opengezet om de vermogens van burgers, zelfstandigen en ondernemers te pluimen. Daarvoor wenst spreker de minister te waarschuwen.

De heer Van Quickenborne vervolgt met het poneren van vijf principiële opmerkingen.

autorité publique qui se concentre sur ses missions principales qu'en un État qui veut tout contrôler et exploite massivement les données des citoyens.

L'argument le plus utilisé en faveur du *money control* est que la très grande majorité des citoyens n'ont de toute façon rien à cacher. Ce ne sont pas des fraudeurs: ils travaillent, ils entreprennent et ils épargnent. Mais jusqu'où peuvent aller les pouvoirs publics dans ce domaine? Ce qu'ils proposent aujourd'hui équivaut à accrocher une caméra au-dessus de chaque compte bancaire de l'ensemble des Belges et des entreprises.

L'intervenant confirme ensuite que toute forme de fraude est condamnable. En l'occurrence, il ne s'agit toutefois pas de cela, mais de placer tous les comptes bancaires de tous les Belges dans le système à des fins de sélection des dossiers. Cela représente une énorme quantité de données. Il s'agirait de 55 millions de comptes bancaires actifs intégrés dans le PCC, auxquels il faudrait ajouter tous les soldes, tous les comptes bancaires des entreprises et tous les contrats financiers. Le PCC contiendrait ainsi un demi-milliard de données. Or, ces données relèvent de la vie privée des citoyens et n'ont jamais été volontairement partagées avec l'administration fiscale. Jusqu'à présent, ces informations relatives aux comptes bancaires ne pouvaient être consultées qu'en cas d'indices de fraude fiscale (article 322 du CIR). Ce principe est maintenant fondamentalement inversé, car toutes les données financières sans distinction seront désormais injectées dans les systèmes du SPF Finances.

Selon l'intervenant, le ministre se défend en affirmant que le *data mining* existe depuis longtemps, mais il concernait jusqu'ici uniquement les données que les citoyens étaient obligés de partager avec l'administration fiscale, par exemple dans le cadre de la déclaration d'impôts. Aujourd'hui, l'administration fiscale va utiliser des données privées que les citoyens ne partagent pas eux-mêmes. M. Van Quickenborne appelle cela le *money control*. L'administration va même engager 377 contrôleurs fiscaux pour réaliser des contrôles supplémentaires et exploiter toutes les données des citoyens. Des milliers de mamies et de papys devront se faire du souci en fin d'année. Cette chasse aux sorcières fiscale traquera tous les Belges. Selon le membre, la mesure est introduite à la demande du partenaire Vooruit pour éviter de devoir créer un cadastre des fortunes. Le but est toutefois d'avoir accès au PCC, car c'est là que toutes les informations financières de tous les Belges sont réunies. Cela ouvre une brèche pour dépouiller les citoyens, les indépendants et les entreprises de leur patrimoine. L'intervenant veut mettre en garde le ministre contre ce risque.

M. Van Quickenborne formule ensuite cinq remarques fondamentales.

Ten eerste wenst hij te weten of alle bankrekeningen van alle Belgen in het systeem zullen terechtkomen.

Ten tweede verwijst spreker naar “de bomma en haar enveloppe” en de bewering van de minister dat deze situatie niet beoogd wordt. Maar als men de wet leest, staat er dat als er een risico is tot het plegen van een inbreuk op een fiscale wet of een reglementering, dat dan de-pseudonimisatie kan plaatsvinden. Er wordt niet gesproken over ernstige of georganiseerde fraude. En er zijn duizenden fiscale wetten en reglementeringen. De minister heeft eerder verklaart dat er geen onderscheid bestaat tussen grote en kleine fraude. Dat is echter niet correct. Er bestaat wel degelijk een verschil tussen gewone fraude enerzijds en ernstige, georganiseerde fraude anderzijds. Artikel 1 van het koninklijk besluit van 9 februari 2020 tot uitvoering van artikel 29, § 4, van het Wetboek van Strafvordering (*Belgisch Staatsblad* van 24 februari 2020). Het lid citeerde het artikel in extenso. Indien de minister zijn wetsontwerp had beperkt tot die gevallen, had dat aanleiding gegeven tot een totaal ander debat. Nu wordt alle fraude over dezelfde kam geschoren en komt de “bomma met de enveloppe” ook in het vizier. Indien dat niet zo is, moet de tekst worden aangepast. Tientallen fiscale experts zijn eveneens die mening toegedaan.

Ten derde vraagt de heer Van Quickenborne aan de minister of er AI wordt gebruikt. Tijdens de eerste lezing heeft de minister verklaard dat er geen AI wordt gebruikt. Het zou de spreker verbazen mochten honderden miljoenen datasets manueel worden verwerkt.

Minister Jambon stelt dat artificiële intelligentie niet het tegenovergestelde is van manueel of gelijkstaat aan IT-matige verwerking van gegevens.

De heer Van Quickenborne vervolgt zijn redenering. Hij verwijst naar de heer Preneel, privacy-expert van de KU Leuven, die stelt dat SAS-software, opgericht in 1972, recent ook actief is geworden op vlak van AI en *machine learning*. Het gebruikt nu AI en zelfs LLM (*large language models*). Dat is minder gesofisticeerd dan Open AI of Anthropic, maar is zeker niet minder privacy-intrusief. Maar de SAS-software van Financiën gebruikt dus wel degelijk AI. Daarnaast verwijst spreker naar een schriftelijke vraag die hij op 24 maart 2025 aan de minister heeft gesteld over het gebruik van datamining door de FOD Financiën. In zijn antwoord stelt de minister dat momenteel VDMML (*Visual Data Mining & Machine Learning*) en E-Miner van het SAS-platform worden gebruikt. Volgens de minister zijn dat geen autonome AI-systemen. Maar de heer Van Quickenborne komt tot de conclusie dat het wel degelijk gaat over AI-systemen en dat AI dus wel wordt gebruikt. Ook in het Strategisch

Premièremment, il voudrait savoir si tous les comptes bancaires de tous les Belges atterrissent dans le système.

Deuxièmement, l'intervenant évoque “la mamie et son enveloppe” et le fait que le ministre affirme ne pas viser cette situation. Néanmoins, il est écrit dans la loi que la dépseudonymisation peut avoir lieu en cas de risque d'infraction à une loi ou réglementation fiscale. Il n'est pas question de fraude grave ou organisée, et il existe des milliers de lois et réglementations fiscales. Le ministre a déclaré précédemment qu'il n'y avait pas de distinction entre la grande fraude et la petite fraude. C'est pourtant faux. Il existe bel et bien une différence entre la fraude ordinaire et la fraude grave, organisée. L'article 1^{er} de l'arrêté royal du 9 février 2020 portant exécution de l'article 29, § 4, du Code d'instruction criminelle (*Moniteur Belge* du 24 février 2020). Le membre a cité l'article in extenso. Si le ministre avait limité son projet de loi à ces cas, le débat aurait été totalement différent. Aujourd'hui, toutes les formes de fraude sont mises dans le même sac, et “l'enveloppe de la mamie” est aussi dans le collimateur. Si telle n'est pas l'intention, il faut modifier le texte. Des dizaines d'experts fiscaux partagent d'ailleurs ce point de vue.

Troisièmement, M. Van Quickenborne demande au ministre si l'intelligence artificielle est utilisée. Lors de la première lecture, le ministre a déclaré que le système n'avait pas recours à l'IA. L'intervenant serait surpris que des centaines de millions d'ensembles de données soient traités manuellement.

Le ministre Jambon précise que l'intelligence artificielle n'est pas le contraire du traitement manuel et ne désigne pas tout traitement informatique de données.

M. Van Quickenborne poursuit son raisonnement. Il se réfère aux propos de M. Preneel, expert en matière de vie privée à la KU Leuven, qui indique que le logiciel SAS, créé en 1972, s'ouvre également depuis peu à l'intelligence artificielle et à l'apprentissage automatique. Le logiciel utilise maintenant l'IA et même de grands modèles de langage. Le système est moins sophistiqué qu'Open AI ou Anthropic, mais il n'est certainement pas moins intrusif sur le plan de la vie privée. Toujours est-il que logiciel SAS du SPF Finances utilise l'intelligence artificielle. Par ailleurs, l'intervenant renvoie à une question écrite qu'il a posée au ministre le 24 mars 2025, en ce qui concerne l'utilisation du *data mining* par le SPF Finances. Le ministre a répondu que l'on utilisait actuellement les systèmes VDMML (*Visual Data Mining & Machine Learning*) et E-Miner de la plateforme SAS. Selon le ministre, ce ne sont pas des systèmes d'IA autonomes, mais M. Van Quickenborne en conclut qu'il s'agit

Plan 2025-2029 van de FOD Financiën wordt verwezen naar het gebruik van artificiële intelligentie : zie blz. 7 en 14 van het Plan : <https://fin.belgium.be/nl/strategisch-plan-en-operationeel-plan>. Het lid citeert deze passages uit het Strategisch Plan.

Ter staving van zijn stelling verwijst het lid naar de verklaringen van een aantal ambtenaren van de FOD Financiën.

De heer Yannic Hulot (Bijzondere Belastinginspectie) verklaarde in L'Echo in 2019, op de vraag van de journalist of dit wapen alle btw-carrousels in Europa kan neutraliseren, het volgende : "Het is een systeem van artificiële intelligentie dat zich baseert op feiten uit het verleden. De fraudeur kan dus nog altijd slagen in een 'one shot', buiten het systeem om."

Op dezelfde manier verklaarde mevrouw Margaux Smets (die 12 jaar werkte bij de Bijzondere Belastinginspectie) in 2023 in het Tijdschrift Beleggingsfiscaliteit : "Er is wel een beperkt aantal dossiers dat geselecteerd wordt met behulp van AI, zoals bijvoorbeeld webshops die niet aan hun verplichtingen hebben voldaan."

De heer Hans D'Hondt, voorzitter van het directiecomité van de FOD Financiën, verklaarde in 2018 in een IOTA-rapport : "Vanaf 2019 willen we automatisch de invorderingsactie selecteren die het meest efficiënt is en machine-learningtechnieken gebruiken. Uiteraard zullen we de actuele modellen blijven bijwerken omdat sommige criteria elk jaar veranderen – het is een doorlopend proces."

De heer Van Quickenborne wijst erop dat de modellen die de heer D'Hondt beschrijft, als gebruikmakend van machine learning – IRIS, Delphi, Hermes en Pegasus – ook worden vermeld in de OECD Tax Administration Series 2019.

Tot slot herinnert de spreker eraan dat de heer Dierickx (BISC, FOD Financiën) expliciet verwijst naar het gebruik van AI voor "auditmining", de term die de FOD Financiën gebruikt voor datamining ten behoeve van controles.

Waarom ontkent de minister dan dat er AI wordt gebruikt?

De heer Dieter Vanbesien (Ecolo-Groen) stelt aan de vorige spreker de vraag wat AI is. Het is een technologie die zichzelf kan verbeteren. Waarom is het dan zo problematisch dat een algoritme voor datamining zichzelf zou kunnen verbeteren?

bel et bien de systèmes d'intelligence artificielle et que l'on utilise donc l'IA. Le Plan stratégique 2025-2029 du SPF Finances mentionne aussi le recours à l'intelligence artificielle : voir pp. 7 et 14 du Plan Stratégique : <https://fin.belgium.be/fr/plan-strategique-et-plan-operationnel>. Le membre cite ces passages du Plan stratégique.

À l'appui de son argumentation, le député renvoie aux déclarations de plusieurs fonctionnaires du SPF Finances.

M. Yannic Hulot (Inspection spéciale des impôts) a déclaré dans L'Echo en 2019, en réponse à la question du journaliste qui lui demandait si cette arme pouvait neutraliser tous les carrousels de TVA en Europe : "Il s'agit d'un système d'intelligence artificielle qui se base sur des faits passés. Le fraudeur peut donc toujours réussir un "one shot", en dehors du système."

De la même manière, Mme Margaux Smets (qui a travaillé pendant 12 ans à l'Inspection fiscale spéciale) a déclaré en 2023 dans le magazine Beleggingsfiscaliteit : "Il existe toutefois un nombre limité de dossiers qui sont sélectionnés à l'aide de l'IA, comme par exemple les boutiques en ligne qui n'ont pas respecté leurs obligations."

M. Hans D'Hondt, président du comité de direction du SPF Finances, a déclaré dans un rapport IOTA en 2018 : "À partir de 2019, nous voulons sélectionner automatiquement la mesure de recouvrement la plus efficace et utiliser des techniques d'apprentissage automatique. Bien entendu, nous continuerons à mettre à jour les modèles actuels, car certains critères changent chaque année — il s'agit d'un processus continu."

M. Van Quickenborne souligne que les modèles décrits par M. D'Hondt comme utilisant l'apprentissage automatique – IRIS, Delphi, Hermes et Pegasus – sont également mentionnés dans la série 2019 de l'OCDE sur l'administration fiscale.

Enfin, l'orateur rappelle que M. Dierickx (BISC, SPF Finances) fait explicitement référence à l'utilisation de l'IA pour l'"audit mining", terme utilisé par le SPF Finances pour désigner l'exploration de données à des fins de contrôle.

Pourquoi le ministre nie-t-il alors toute utilisation de l'IA?

M. Dieter Vanbesien (Ecolo-Groen) demande à l'intervenant précédent ce qu'est l'intelligence artificielle. C'est une technologie qui peut s'améliorer d'elle-même. Pourquoi est-ce donc si problématique qu'un algorithme de *data mining* puisse s'améliorer de lui-même?

De heer Mathieu Michel (MR) wijst op een cruciaal verschil tussen enerzijds algemene AI-algoritmes die een black box zijn en waarvan men niet weet hoe ze werken, en anderzijds particuliere algoritmes waarvan men wel weet hoe ze functioneren en waarom bepaalde keuzes worden gemaakt. Deze laatste kunnen worden gecontroleerd en zijn dus democratischer.

De heer Dieter Vanbesien (Ecolo-Groen) voegt daar nog aan toe dat de gebruiker van VDMML de ingevoerde algoritmes zelf kan formuleren. Het gaat dus niet over een black box.

De heer Lode Vereeck (VB) wijst ook op de discrepantie in de verklaringen van de minister en vraagt hem of hij moet begrijpen dat de FOD Financiën zal blijven gebruik maken van de oude versie van SAS die geen gebruik maakt van AI.

De heer Vincent Van Quickenborne (Open Vld) vraagt vervolgens aan de minister welke versie van SAS wordt gebruikt. Hij heeft immers bij het consulteren van de DAM-fiches gezien dat wel degelijk de *AI-enabled* versie wordt gebruikt. En dat is volgens hem problematisch omdat ook een semi-autonoom systeem kan evolueren naar een black box. Bovendien kan elk AI-systeem hallucineren. Burgers zullen dus onterecht kunnen worden beschuldigd van fraude. De waarborgen voorzien in de Europese AI-act moeten dus worden toegepast om te zorgen voor de nodige transparantie.

Ten vierde verwijst de heer Van Quickenborne naar de menselijke tussenkomst. Het probleem is de timing van de tussenkomst, die pas gebeurt nadat de geautomatiseerde resultaten van datamining gedeeld zijn met de controlediensten. Zij beslissen dan over de eventuele opstart van een onderzoek. De spreker stelt dat het hier gaat over een *ex post* en passief controlesysteem, wat niet conform is aan de regels van de AVG (Algemene verordening gegevensbescherming). Artikel 22 van de AVG voorziet immers in een voorafgaandelijke menselijke tussenkomst.

Ten vijfde wijst de heer Van Quickenborne op het gebrek aan controlemogelijkheden door de belastingplichtige op de door de administratie gebruikte parameters en de algoritmes. De DAM-fiche is immers niet raadpleegbaar door de belastingplichtige. Hoe kan die zich verdedigen tegen een beschuldiging waarvan hij niet weet op welke grondslag ze is gemaakt? De minister heeft zelf verklaard dat de criteria en risicoprofielen gebruikt door de FOD Financiën worden gedocumenteerd door de DAM-fiches. Die laatste maken echter deel uit van de interne strategie van het beheer van de risico's en zijn niet bestemd voor externe verdeling. Dat alles gebeurt

M. Mathieu Michel (MR) insiste sur la différence essentielle qui existe entre, d'une part, les algorithmes d'IA génériques, qui sont une boîte noire dont on ignore le fonctionnement et, d'autre part, les algorithmes spécifiques, dont on comprend le fonctionnement et les raisons de certains choix. Les algorithmes spécifiques peuvent être contrôlés et sont donc plus démocratiques.

M. Dieter Vanbesien (Ecolo-Groen) ajoute encore que l'utilisateur de VDMML peut formuler lui-même les algorithmes introduits. Il ne s'agit donc pas d'une boîte noire.

M. Lode Vereeck (VB) relève aussi des contradictions dans les déclarations du ministre et il lui demande s'il faut comprendre que le SPF Finances continuera d'utiliser l'ancienne version de SAS qui n'utilise pas l'IA.

M. Vincent Van Quickenborne (Open Vld) demande ensuite au ministre quelle version de SAS est utilisée. En effet, en consultant les fiches DAM, il a remarqué que la version intégrant l'IA était bel et bien utilisée. Selon lui, cela pose problème parce qu'un système semi-autonome peut aussi évoluer pour devenir une boîte noire. En outre, tout système d'IA peut avoir des hallucinations. Les citoyens pourront donc être accusés de fraude à tort. Par conséquent, il convient d'appliquer les garanties prévues dans la législation européenne sur l'intelligence artificielle afin d'assurer la transparence nécessaire.

Quatrièmement, M. Van Quickenborne évoque l'intervention humaine. Le problème concerne le moment de l'intervention, qui n'a lieu qu'après que les résultats automatisés du *data mining* ont été partagés avec les services de contrôle. Ces derniers décident ensuite du lancement éventuel d'une enquête. Selon l'intervenant, il s'agit en l'occurrence d'un système de contrôle passif *ex post*, ce qui n'est pas conforme au règlement général sur la protection des données (RGPD), dont l'article 22 prévoit une intervention humaine préalable.

Cinquièmement, M. Van Quickenborne souligne que le contribuable n'a aucune possibilité de contrôler les paramètres et les algorithmes utilisés par l'administration. En effet, la fiche DAM n'est pas accessible au contribuable. Comment peut-il alors se défendre contre une accusation dont il ignore le fondement? Le ministre a lui-même déclaré que les critères et les profils de risques utilisés par le SPF Finances étaient documentés par les fiches DAM. Ces dernières font toutefois partie de la stratégie interne de la gestion des risques et ne sont pas destinées à une distribution externe. Ce mécanisme est mis en œuvre sans que le contribuable

dus zonder dat de belastingplichtige weet waarom hij of zij wordt geselecteerd. Spreker stelt dat het gaat om Chinese praktijken waarbij iemand wordt beschuldigd van iets, maar de bewijzen daarvoor worden niet getoond. Hij verwijst daarbij ook naar de Antigoon-doctrine die stelt dat vormfouten slechts aanleiding kunnen geven tot nietigheid van een besluit, indien dit uitdrukkelijk in de wetgeving wordt omschreven. En dat is een fundamenteel probleem.

De heer Van Quickenborne legt vervolgens een reeks vragen voor aan de minister.

Klopt het dat alle bankrekeningen van 11 miljoen Belgen in de datawarehouse zullen terechtkomen? Gaat het om 55 miljoen bankrekeningen d.d. 31 december 2024? Waarom beperkt de minister het mechanisme niet tot ernstige en georganiseerde fraude zoals bepaald in het koninklijk besluit van 9 januari 2020 tot uitvoering van artikel 29, § 4, van het Wetboek van Strafvordering? Wordt er A.I. gebruikt of niet? Waarom wordt de selectie overgelaten aan een computer zonder voorafgaande menselijke tussenkomst? Waarom mag de belastingplichtige niet weten waarom hij werd geselecteerd?

De spreker is verder van mening dat de wettekst voor een stuk van amateurisme getuigt. Oorspronkelijk zat het "*money control*"-systeem vervat in de programmatwet. Nu wordt het via een amendement ingevoerd en moet het terechtkomen in een nieuwe paragraaf 3 van artikel 5 van de wet van 3 augustus 2012 houdende bepalingen betreffende de verwerking van persoonsgegevens door de Federale Overheidsdienst Financiën in het kader van zijn opdrachten.

De tweede alinea van de nieuwe bepaling stelt: "Onverminderd de bewaring noodzakelijk voor de verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden bedoeld in artikel 89 van de algemene verordening gegevensbescherming, worden de persoonsgegevens die voortkomen uit de verwerkingen in het datawarehouse niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor zij werden verwerkt, met een maximale bewaartermijn die één jaar na de verjaring van alle vorderingen die tot de bevoegdheid van de verwerkingsverantwoordelijke behoren en, in voorkomend geval, de definitieve beëindiging van de administratieve en rechterlijke procedures en rechtsmiddelen en de integrale betaling van alle hiermee verbonden bedragen niet mag overschrijden." (DOC 56 0963/005, amendement nr. 16, blz. 11).

Het lid merkt op dat deze alinea reeds voorkomt in artikel 5 van de wet van 2012 zoals gewijzigd door artikel 71 van de wet van 5 september 2018 tot oprichting

sache pourquoi il est sélectionné. Selon l'intervenant, ces méthodes s'apparentent à des pratiques chinoises, consistant à accuser une personne d'un délit sans en présenter les preuves. À cet égard, il se réfère aussi à la doctrine Antigone, selon laquelle des vices de forme ne peuvent entraîner la nullité d'une décision que si cela est explicitement défini dans la législation. Cela pose un problème fondamental.

M. Van Quickenborne adresse ensuite une série de questions au ministre.

Est-il vrai que les comptes bancaires des 11 millions de Belges seront tous enregistrés dans la *datawarehouse*? S'agit-il de 55 millions de comptes bancaires au 31 décembre 2024? Pourquoi le ministre ne limite-t-il pas le mécanisme à la fraude grave et organisée, comme le prévoit l'arrêté royal du 9 janvier 2020 portant exécution de l'article 29, § 4, du Code d'instruction criminelle? L'intelligence artificielle sera-t-elle utilisée? Pourquoi la sélection sera-t-elle confiée à un ordinateur, sans intervention humaine? Pourquoi le contribuable n'aura-t-il pas le droit de savoir pourquoi il a été sélectionné?

L'intervenant estime, en outre, que le texte de loi témoigne d'un certain amateurisme. À l'origine, le système du *money control* était inclus dans la loi-programme mais il est aujourd'hui introduit par un amendement et doit faire l'objet d'un nouveau § 3 inséré dans l'article 5 de la loi du 3 août 2012 portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions.

L'alinéa 2 de la nouvelle disposition s'énonce comme suit: "Sans préjudice de la conservation nécessaire pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques visé à l'article 89 du règlement général sur la protection des données, les données à caractère personnel qui résultent des traitements dans le datawarehouse ne sont pas conservées plus longtemps que nécessaire au regard des finalités pour lesquelles elles sont traitées, avec une durée maximale de conservation ne pouvant excéder un an après la prescription de toutes les actions qui relèvent de la compétence du responsable du traitement et, le cas échéant, la cessation définitive des procédures et recours administratifs et judiciaires ainsi que du paiement intégral de tous les montants y liés." (DOC 56 0963/005, amendement n° 16, p. 11).

Le membre fait observer que cet alinéa figure déjà à l'article 5 de la loi de 2012, telle que modifiée par l'article 71 de la loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant

van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG. Deze wet werd gepubliceerd in het *Belgisch Staatsblad* van 10 september 2018. Hij verzoekt de minister om deze alinea te schrappen via een amendement.

De spreker wijst vervolgens op een tegenstrijdigheid tussen de eerste alinea van datzelfde amendement en de verantwoording. In de eerste alinea lijkt er sprake te zijn van bulkverwerking van gegevens, terwijl de verantwoording eerder wijst op een verwerking op basis van toegelaten aanvragen, zoals blijkt uit de passage: “Om de beoogde gegevens te kunnen verwerken, worden de gegevens geëxtraheerd uit het CAP via toegelaten aanvragen en na overleg met de Data Protection Officers (hierna: “DPO”) van de NBB en de FOD Financiën (...). (DOC 56 0963/005, amendement nr. 16, blz. 15)” Bij bulkverwerking gaat het om een verwerking in één keer, terwijl het andere scenario een gerichte informatiebron betreft. Hoe moet men dit nu lezen?

Uit de toelichting blijkt dat het CAP-systeem geen volautomatisch systeem is. Er is altijd een menselijke tussenkomst die bepaalt of een dossier onderzocht wordt of niet. In de zesde alinea van het amendement nr. 16 valt echter te lezen: “*Indien een depseudonimisatie plaats heeft, zal vervolgens aan de bevoegde controledienst worden gevraagd om een controle van het geselecteerde dossier uit te voeren.*” Waarom wordt in deze alinea het werkwoord “zal” en niet “kan” gebruikt? Volgens de spreker gaat het hier niet langer om een menselijke beslissing, maar om de louter administratieve uitvoering van een door een algoritme gegenereerd signaal.

Het Kamerlid vat nog eens de procedure van het “money control”-systeem samen. Eerst vindt een automatische analyse plaats van miljoenen records, zonder voorafgaande menselijke selectie. Alle in het CAP opgenomen gegevens worden gepseudonimiseerd, geanalyseerd en getoetst aan profielen van potentiële fraudeurs. Vervolgens wordt dit profiel toegepast op de gegevens van alle burgers om risicodossiers te identificeren. Het gaat dus om twee afzonderlijke maar onderling verbonden gegevensverwerkingen waaraan alle Belgische burgers worden onderworpen. De spreker verneemt graag of dit klopt en vraagt de minister om zelf alle stappen uiteen te zetten.

diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE. Cette loi a été publiée dans le *Moniteur belge* du 10 septembre 2018. Par conséquent, il demande au ministre de supprimer cet alinéa par voie d'amendement.

L'intervenant attire ensuite l'attention sur une contradiction entre l'alinéa 1^{er} dudit amendement et sa justification. Dans cet alinéa, il semble être question d'un traitement de données en masse, tandis que la justification évoque plutôt, dans le passage suivant, un traitement sur la base de demandes autorisées: “Afin de pouvoir procéder au traitement de données envisagé, les données sont extraites du PCC via des demandes autorisées et après concertation avec les délégués à la protection des données (ci-après: “DPO”) de la BNB et du SPF Finances (...)” (DOC 56 0963/005, amendement n° 16, p. 15) Le traitement en masse consiste en un traitement unique, tandis que, dans l'autre scénario, il est question d'une source d'information ciblée. Comment faut-il interpréter cela?

Il ressort de l'exposé des motifs que le système du PCC n'est pas entièrement automatisé. C'est toujours à l'issue d'une intervention humaine qu'il est décidé si un dossier doit être examiné ou pas. Toutefois, l'alinéa 6 de l'amendement n° 16 s'énonce comme suit: “Si une depseudonymisation est réalisée, il sera alors demandé au service de contrôle compétent d'effectuer une vérification du dossier sélectionné.” Pourquoi ce passage contient-il les mots “sera alors demandé” et pas les mots “pourra alors être demandé”? Selon l'intervenant, il ne sera plus question d'une décision humaine, mais bien de la simple exécution administrative d'un signal généré par un algorithme.

Le membre résume à nouveau la procédure du système de money control. Tout d'abord, une analyse automatique est effectuée sur des millions de dossiers, sans sélection humaine préalable. Toutes les données enregistrées dans le PCC sont pseudonymisées, analysées et comparées à des profils de fraudeurs potentiels. Ce profil est ensuite appliqué aux données de tous les citoyens afin d'identifier les dossiers à risque. Tous les citoyens belges sont donc soumis à deux traitements de données distincts mais interdépendants. L'intervenant souhaite savoir si cette interprétation est correcte et demande au ministre d'exposer lui-même toutes les étapes.

Hij kondigt voorts aan amendementen te zullen indienen.

De spreker verneemt verder graag of het klopt dat de minister de CAP-wetgeving wenst aan te passen, en zo ja wat in dat wetsontwerp staat.

Het lid begrijpt niet waarom de minister, ondanks de aanzienlijke tegenkanting in de samenleving tegen dit project, vastberaden lijkt om het alsnog door te voeren. Staan de parlementsleden van zowel de meerderheid als de oppositie zo veraf van het volk dat dit project er per se door moet?

De spreker ziet evenwel nog hoop in het feit dat Vlaams Parlements lid, mevrouw Nadia Sminate (N-VA) zich publiek heeft uitgesproken tegen "*money control*". Dat blijkt uit een audiofragment dat hij afspeelt. Wie heeft gelijk: mevrouw Sminate of de socialisten? Wat vindt de minister van de opmerkingen van zijn partijgenote? De minister kan "*money control*" toch onmogelijk aanvaarden? Het is een hold-up van de socialisten waar de minister zich tegen moet verzetten, meent het lid.

De heer Steven Matheï (cd&v) verwijst naar de eerste lezing wat betreft de bepalingen van de wet. Met betrekking tot het CAP benadrukt hij dat de bestrijding van fiscale fraude essentieel is en op een zo efficiënt mogelijke wijze moet gebeuren, met de nodige waarborgen.

Het lid merkt op dat in het debat vaak verschillende zaken op één hoop worden gegooid. Het CAP, zoals sinds 2022 voorzien, met raadpleegbare saldi die kunnen worden opgevraagd, blijft ongewijzigd. Het wordt enkel uitgebreid met crypto- en effectenrekeningen. De saldi van deze rekeningen zullen in het CAP worden opgenomen, wat iets heel anders is dan het live volgen van bankapps, zoals werd gesuggereerd.

Het CAP kent twee onderscheiden toepassingen: raadpleging enerzijds en datamining anderzijds.

De raadpleging van het CAP door ambtenaren gebeurt onder strikte voorwaarden, zoals vastgelegd in artikel 322 WIB 92. Het vereist een vermoeden van fraude en is sterk gereguleerd. Dat blijft ook zo.

Bij datamining is het essentieel het onderscheid te maken tussen selectie en controle. Selectie gebeurt anoniem en volgens een vooraf vastgelegde procedure, met een eerste menselijke tussenkomst. Pas wanneer

Il ajoute qu'il déposera des amendements.

Il souhaite également savoir s'il est exact que le ministre entend modifier la législation relative au PCC et, le cas échéant, ce que prévoit le projet de loi.

Le membre ne comprend pas pourquoi le ministre, malgré la forte opposition de la société à ce projet, semble déterminé à le mettre en œuvre. Les membres de la majorité comme ceux de l'opposition sont-ils à ce point éloignés du peuple pour vouloir faire aboutir ce projet à tout prix?

Il voit toutefois encore de l'espoir dans le fait qu'une membre du Parlement flamand, Mme Nadia Sminate (N-VA), se soit publiquement opposée au *money control*, comme l'atteste un extrait audio qu'il diffuse. Qui a raison: Mme Sminate ou les socialistes? Que pense le ministre des observations formulées par sa collègue de parti? Le ministre ne peut tout de même pas accepter le *money control*. Il estime qu'il s'agit d'un coup de force des socialistes auquel le ministre doit s'opposer.

M. Steven Matheï (cd&v) renvoie à la première lecture en ce qui concerne les dispositions de la loi. S'agissant du PCC, il souligne que la lutte contre la fraude fiscale est essentielle et qu'il convient de la mener aussi efficacement que possible, tout en appliquant les garanties nécessaires.

Le membre fait observer que différentes questions ont souvent été mêlées au cours du débat. Le PCC, qui permet la consultation des soldes depuis 2022, reste inchangé, si ce n'est qu'il sera étendu aux comptes de cryptomonnaies et aux comptes-titres. Les soldes de ces comptes seront donc intégrés au PCC, ce qui n'a absolument rien à voir avec le fait de suivre les applications bancaires des contribuables en temps réel, comme d'aucuns l'ont suggéré.

Le PCC permet deux applications distinctes: d'une part, la consultation, et d'autre part, le *data mining*.

Les agents de l'administration consultent le PCC dans le respect de conditions strictes visées à l'article 322 du CIR92. La consultation est très encadrée: elle requiert notamment une suspicion de fraude. Le projet de loi à l'examen n'apporte aucune modification en la matière.

Dans le cadre du *data mining*, il est essentiel d'opérer une distinction entre la sélection et le contrôle. La sélection est anonyme et résulte d'une procédure définie au préalable qui prévoit une première intervention

een selectie een *hit* oplevert, wordt deze overgemaakt voor controle.

Dat onderscheid is essentieel om privacy te beschermen, stelt het lid. Het vermoeden van fraude hoort niet in de selectie, want anders worden beide processen vermengd.

Tot slot merkt de spreker op dat, volgens het wetsontwerp, effecten- en cryptorekeningen vanaf 31 december 2025 aan het CAP worden toegevoegd. Is dit tijdschema afgestemd met de banken en haalbaar?

De heer Niels Tas (Vooruit) benadrukt dat solidariteit, waarbij iedereen een eerlijke bijdrage levert, de basis vormt van onze welvaartsstaat. Daarom is een effectieve en efficiënte bestrijding van fiscale fraude noodzakelijk.

Het lid stelt dat burgers het vanzelfsprekend vinden dat de overheid alles in het werk stelt om fiscale fraude op te sporen. Zij dragen immers een aanzienlijk deel van hun inkomen af aan belastingen. Het spreekt voor zich dat de overheid erop toeziet dat iedereen een eerlijke bijdrage levert en dat fraudeurs en criminelen worden aangepakt, zodat ook zij eerlijk bijdragen.

De nieuwe wetgeving stelt het CAP-systeem in staat om fiscale fraude veel efficiënter en doelgerichter op te sporen. Het lid benadrukt dat de fiscus moet meegaan met de digitalisering: fraude opsporen gebeurt niet langer met pen en papier, maar met moderne technologie. Door een betere dossierselectie zullen gewone belastingplichtigen nu minder gecontroleerd worden, terwijl fraudeurs die hun bijdrage proberen te ontlopen een grotere kans op controle hebben.

Het lid benadrukt dat menselijke tussenkomst in het proces behouden blijft. Een beperkte groep *dataminers* krijgt toegang tot gepseudonimiseerde gegevens uit het CAP en kan deze koppelen aan fiscale gegevens. Daarna volgt een beoordeling door de controledienst, waarna het dossier pas met identificatie naar de fiscus gaat. Het lid stelt dat dit geen automatisch proces is en verwijst daarbij naar de DAM-fiches.

Hij verwerpt vervolgens de suggestie dat het systeem neerkomt op live meekijken in bankapps. Het gaat om

humaine. Ce n'est que lorsqu'une sélection donne un résultat (*hit*) que le dossier concerné est transmis en vue d'un contrôle.

Selon l'intervenant, cette distinction est essentielle en vue de la protection de la vie privée. La suspicion de fraude ne joue aucun rôle dans la phase de sélection; dans le cas contraire, il y aurait confusion entre les deux processus.

Le membre conclut son intervention en soulignant que le projet de loi prévoit l'intégration des comptes-titres et des comptes de cryptomonnaies au PCC dès le 31 décembre 2025. Ce calendrier est-il réaliste et a-t-il fait l'objet d'une concertation avec le secteur bancaire?

M. Niels Tas (Vooruit) souligne que la solidarité, qui repose sur les contributions équitables de chacun, constitue le fondement de notre État-providence. C'est pourquoi il est nécessaire de lutter effectivement et efficacement contre la fraude fiscale.

Selon l'intervenant, les citoyens considèrent qu'il est évident que les pouvoirs publics mettent tout en œuvre pour détecter la fraude fiscale. Ils consacrent en effet une part importante de leurs revenus au paiement des impôts. Par ailleurs, il est également parfaitement normal que les pouvoirs publics veillent à ce que chacun contribue équitablement et à ce que les fraudeurs et les criminels soient démasqués afin qu'ils contribuent eux aussi de manière équitable.

La nouvelle législation permettra au système du PCC de détecter la fraude fiscale de façon nettement plus efficace et ciblée. Le membre souligne que l'administration fiscale doit suivre l'évolution numérique: on ne détecte plus la fraude en utilisant un stylo et du papier, mais les technologies modernes. Grâce à l'amélioration du processus de sélection des dossiers, les contribuables ordinaires seront dorénavant moins contrôlés, tandis que les fraudeurs qui tentent de se soustraire à l'impôt auront plus de chances d'être soumis à un contrôle.

L'intervenant souligne que le processus prévoit toujours une intervention humaine. Un groupe limité de *dataminers* pourra accéder aux données pseudonymisées issues du PCC et les associer aux données fiscales. Le dossier sera ensuite soumis au service de contrôle et ce n'est qu'au moment où il est transmis à l'administration fiscale que le contribuable sera identifié. Le membre indique qu'il ne s'agit donc pas d'un processus automatisé et il renvoie à cet égard aux fiches DAM.

Il rejette ensuite l'affirmation selon laquelle le nouveau système permettrait de suivre les applications bancaires

gerichte opsporing van grote fraudeurs, niet om individuele verrichtingen.

De spreker wijst er dan op dat dergelijke technologie in andere landen al miljoenen oplevert en dat dit essentieel is om middelen te vrijwaren voor wie ze nodig heeft.

Hij begrijpt niet waarom sommigen zich verzetten tegen een systeem dat eerlijke belastingen bevordert en rijke fraudeurs aanpakt.

De heer Wouter Vermeersch (VB) richt een reeks vragen tot de minister.

1. DBI en groepsbijdrage – EU-dividenden – onmiddellijke inwerkingtreding door arrest Hof van Justitie

Het Hof van Justitie van de Europese Unie oordeelde dat het aftrekverbod van het huidige artikel 206/3, § 1, 8^e, WIB 92 strijdig is met de Europese Moeder-Dochterrichtlijn¹² voor zover dat aftrekverbod de mogelijkheid ontnemt om ontvangen groepsbijdragen te compenseren met de DBI-aftrek voor dividenden van Europese oorsprong (HvJ EU, 13 maart 2025, C-135/24, John Cockerill t. Belgische Staat). Het arrest John Cockerill ligt volledig in lijn met de uitspraak die het Hof deed in de zaken Brussels Securities (C-389/18) en Allianz Belgium (C-295/21).

Om daaraan tegemoet te komen wordt via dit wetsontwerp artikel 206/3, § 1, WIB 92 gewijzigd, zodat de DBI-aftrek voor dividenden van het jaar zelf (art. 205, § 2, WIB 92) kan worden toegepast op het deel van het bedrag van de ontvangen groepsbijdragen, zoals bedoeld in artikel 185, § 4, eerste lid, WIB 92, dat hoger is dan het negatieve resultaat dat werd vastgesteld voor de opname van de groepsbijdrage in de belastbare grondslag van het belastbaar tijdperk.

Er is geen specifieke inwerkingtreding voorzien voor die wetsoepassing. In de memorie van toelichting wordt dat verantwoord door te verwijzen naar de directe werking van de Europese Moeder-Dochterrichtlijn en naar de bindende werking van het arrest John Cockerill.

Echter, het toepassingsgebied van de Europese Moeder-Dochterrichtlijn en dat van het aftrekverbod, waarbij geen onderscheid wordt gemaakt tussen Europese, niet-Europese en Belgische dividenden, loopt niet gelijk.

¹² Richtlijn 2011/96/EU van de Raad van 30 november 2011 betreffende de gemeenschappelijke fiscale regeling voor moedermaatschappijen en dochterondernemingen uit verschillende lidstaten.

en temps réel. L'objectif est la détection ciblée des grands fraudeurs, pas le contrôle des opérations individuelles.

L'intervenant indique que la technologie visée rapporte déjà des millions d'euros dans d'autres pays, ce qui est essentiel pour garantir que les moyens soient alloués à ceux qui en ont besoin.

Il ne comprend pas pourquoi certains membres s'opposent à un système qui favorise une fiscalité équitable et lutte contre la fraude des plus riches.

M. Wouter Vermeersch (VB) adresse une série de questions au ministre.

1. RDT et transfert intra-groupe – dividendes européens – entrée en vigueur immédiate par suite de l'arrêt de la Cour de Justice

La Cour de Justice de l'Union européenne a jugé que l'interdiction de déduction prévue à l'actuel article 206/3, § 1^{er}, 8^e tiret, du CIR92, était contraire à la directive européenne mères-filiales¹² en ce qu'elle prive de la possibilité de compenser les transferts intra-groupe perçus en utilisant la déduction RDT pour les dividendes d'origine européenne (CJUE, 13 mars 2025, C-135/24, John Cockerill c. État belge). Cet arrêt s'inscrit dans le droit fil des décisions que la Cour a déjà rendues dans les affaires Brussels Securities (C-389/18) et Allianz Belgium (C-295/21).

Pour s'y conformer, le projet de loi à l'examen modifie l'article 206/3, § 1^{er}, du CIR92, afin que la déduction RDT des dividendes de l'exercice d'imposition (art. 205, § 2, du CIR92) puisse s'appliquer à la partie du montant des transferts intra-groupe perçus, visés à l'article 185, § 4, alinéa 1^{er}, du CIR92, excédant le résultat négatif établi avant la reprise des transferts intra-groupe repris dans la base imposable de la période imposable.

Aucune date d'entrée en vigueur spécifique n'est prévue pour la modification de la législation précitée, ce qui est justifié dans l'exposé des motifs par l'effet direct de la directive européenne mères-filiales et par l'effet contraignant de l'arrêt John Cockerill.

Cependant, les champs d'application de la directive européenne mères-filiales et de l'interdiction de déduction, qui ne prévoit pas de distinction entre les dividendes européens, non européens et belges, ne sont pas identiques.

¹² Directive 2011/96/UE du Conseil du 30 novembre 2011 concernant le régime fiscal commun applicable aux sociétés mères et filiales d'États membres différents.

Bij de niet-Europese dividenden geldt, als er geen uitdrukkelijke inwerkingtreding is voorzien, dat de maatregel van kracht is vanaf de 10^e dag na publicatie van de wet in het *Belgisch Staatsblad*.

Indien een Belgische moedervereniging een dividend ontvangt van een Britse dochtervereniging, dus buiten de Europese Unie en niet gedekt door de Europese Moeder-Dochterrichtlijn, en daarnaast een groepsbijdrage ontvangt die groter is dan het fiscale verlies, klopt het dat het aftrekverbod niet zal spelen op die Britse dividenden die worden ontvangen na de 10^e dag na publicatie van de wet in het *Belgisch Staatsblad* of voor aangiftes die ingediend worden na de 10^e dag na publicatie van de wet in het *Belgisch Staatsblad*? Hoe ziet de minister de inwerkingtreding van het niet-toepassen van het aftrekverbod voor dividenden uit niet-EU-landen?

2. Belastingkrediet voor aangroei van eigen middelen bij winsten- en batenbehalers in de personenbelasting

Overeenkomstig artikel 289bis WIB 92 wordt vanaf aanslagjaar 2026 aan rijksinwoners die winst of baten behalen een belastingkrediet verleend van 20 %, met een maximum van 7500 euro, van het meerdere van:

— het op het einde van het belastbare tijdperk bestaande positieve verschil tussen de fiscale waarde van de in artikel 41 vermelde vaste activa en het totale bedrag van de schulden met een oorspronkelijke looptijd van meer dan één jaar die betrekking hebben op uitgeoefende beroepswerkzaamheden die winst of baten opbrengen;

— ten opzichte van het op het einde van één van de drie voorafgaande belastbare tijdperken bereikte hoogste bedrag van dit verschil.

Hoe moet de fiscale waarde van een beroepsmatig gebruikte personenwagen bepaald worden? Moet voor de berekening van de fiscale waarde als uitgangspunt rekening worden gehouden met de volledige beroepsmatige aanschaffingsprijs, inclusief de aanschaffingsprijs met betrekking tot het woon-werkverkeer van de winsten- of batenbehalter? En moet deze aanschaffingswaarde verminderd worden met de afschrijvingen die werkelijk zijn aangenomen – de zuivere beroepskilometers vóór de fiscale CO₂-beperking van artikelen 66 en 550 WIB 92 – en die “theoretisch” zijn aangenomen, met betrekking tot het woon-werkverkeer van de winsten- of batenbehalter?

En ce qui concerne les dividendes non européens, si aucune date d'entrée en vigueur spécifique n'est prévue, la mesure entrera en vigueur le 10^e jour de la publication de la loi au *Moniteur belge*.

Si une société mère belge perçoit un dividende d'une filiale britannique, qui se situe donc en dehors de l'Union européenne et qui ne relève pas du champ d'application de la directive européenne mères-filiales, ainsi qu'un transfert intra-groupe excédant la perte fiscale, est-il correct d'affirmer que l'interdiction de déduction ne s'appliquera pas aux dividendes britanniques perçus après le 10^e jour de la publication de la loi au *Moniteur belge* ni aux déclarations introduites après le 10^e jour de la publication de la loi au *Moniteur belge*? Quelle est, selon le ministre, la date d'entrée en vigueur de la non-application de l'interdiction de déduction pour les dividendes d'origine non européenne?

2. Crédit d'impôt pour l'accroissement des fonds propres accordé aux attributaires de bénéfices et de profits à l'impôt des personnes physiques

L'article 289bis du Code des impôts sur les revenus 1992 prévoit d'imputer aux habitants du Royaume qui ont produit des bénéfices ou des profits, à partir de l'exercice d'imposition 2026, un crédit d'impôt de 20 %, pour un montant maximum de 7500 euros, de l'excédent que représente:

— la différence positive existant, à la fin de la période imposable, entre la valeur fiscale des immobilisations visées à l'article 41 et le montant total des dettes dont le terme initial est supérieur à un an, affectées à l'exercice d'activités professionnelles produisant des bénéfices ou des profits;

— par rapport au montant le plus élevé atteint par cette différence, à la fin d'une des trois périodes antérieures.

Comment la valeur fiscale d'une voiture utilisée à des fins professionnelles doit-elle être déterminée? Faut-il, pour calculer cette valeur, se baser sur le prix d'achat professionnel total, y compris le prix d'achat lié aux déplacements entre le domicile et le travail de l'attributaire des bénéfices ou des profits? Et cette valeur d'acquisition doit-elle être diminuée des amortissements réellement admis – kilomètres purement professionnels avant la limitation fiscale des émissions de CO₂ prévue aux articles 66 et 550 du CIR92 – et qui sont “théoriquement” admis, en ce qui concerne les trajets domicile-travail de l'attributaire des bénéfices ou profits?

3. Opsplitsing forfaitaire vergoeding voor dienstverplaatsingen

Werkgevers kunnen een forfaitaire vergoeding voor dienstverplaatsingen met de eigen personenwagen van de werknemer toekennen volgens het overheidsbarema.

Als die werknemer die verplaatsingen doet met zijn eigen plug-in personenwagen aangeschaft in 2026, en de werkgever-éénmanszaak kent die forfaitaire vergoeding voor dienstverplaatsing toe, hoe moet de werkgever-éénmanszaak dan die forfaitaire vergoeding opsplitsen in 2026 tussen elektriciteits-, brandstof- en andere autokosten?

De vraag rijst omdat de fiscale aftrekbaarheid voor de werkgever verschilt per kostencategorie: elektriciteitskosten zijn 100 % aftrekbaar, brandstofkosten maximaal 50 % en andere autokosten volgens de aanpaste gramformule.

4. Opsplitsing voordeel van alle aard

Hoe moet het voordeel van alle aard van een plug-in hybride personenwagen aangeschaft in 2026 gesplitst worden over elektriciteits-, brandstof- en andere autokosten, wanneer een werkgever – éénmanszaak een plug-in hybride ook voor privégebruik ter beschikking stelt van een werknemer?

5. Kostenforfait woon-werkverkeer 0,15 euro/km

Dit wetsontwerp wijzigt artikel 66, § 4, WIB 92 in die zin dat vanaf het aanslagjaar 2027 verbonden aan een belastbaar tijdperk dat ten vroegste aanvangt op 1 januari 2026, het kostenforfait van 0,15 euro/km woon-werkverkeer niet meer van toepassing is voor voertuigen waarvan de beroepskosten overeenkomstig paragraaf 1 niet aftrekbaar zijn.

Betekent dit dat vanaf aanslagjaar 2027 (inkomstenjaar 2026) in de personenbelasting de kostenafrek van 0,15 euro/km voor woon-werkverkeer met de eigen auto, niet meer aftrekbaar is voor voertuigen waarvan de beroepskosten (werk-werkverkeer) andere dan elektriciteits- en brandstofkosten overeenkomstig de algemene regeling niet aftrekbaar zijn vanaf aanslagjaar 2027? En dat dus, in tegenstelling daarmee, het kostenforfait van 0,15 euro/km voor woon-werkverkeer vanaf aanslagjaar 2027 enkel nog geldt indien het gaat om een voertuig waarvan de “algemene” kosten – de

3. Ventilation de l'indemnité forfaitaire pour les déplacements professionnels

Les employeurs peuvent accorder une indemnité forfaitaire pour les déplacements professionnels que le travailleur effectue avec sa propre voiture, conformément au barème du secteur public.

Si le travailleur effectue ces déplacements avec sa propre voiture rechargeable achetée en 2026 et que l'employeur-entrepreneur individuel accorde cette indemnité forfaitaire pour les déplacements professionnels, comment l'employeur-entrepreneur individuel devra-t-il ventiler cette indemnité forfaitaire en 2026 entre les frais d'électricité, les frais de carburant et les autres frais?

La question se pose dès lors que la déductibilité fiscale pour l'employeur diffère en fonction de la catégorie de frais: les frais d'électricité sont déductibles à 100 %, les frais de carburant à concurrence de 50 % au maximum tandis que les autres frais de voiture sont déductibles selon la formule adaptée du nombre de grammes de CO₂.

4. Ventilation de l'avantage de toute nature

Comment l'avantage de toute nature d'une voiture hybride rechargeable achetée en 2026 doit-il être ventilé entre les frais d'électricité, les frais de carburant et les autres frais lorsqu'un employeur-entrepreneur individuel met également une voiture hybride rechargeable à la disposition d'un travailleur pour son usage privé?

5. Forfait de frais de 0,15 euro par kilomètre parcouru entre le domicile et le lieu travail

Le projet de loi à l'examen modifie l'article 66, § 4, du Code des impôts sur les revenus 1992 en ce sens qu'à compter de l'exercice d'imposition 2027, pour une période imposable qui débutera au plus tôt le 1^{er} janvier 2026, le forfait de frais de 0,15 euro par kilomètre parcouru entre le domicile et le lieu de travail ne s'appliquera plus aux véhicules ne donnant plus lieu à une déductibilité des frais professionnels conformément au paragraphe 1^{er}.

Cela signifie-t-il qu'à partir de l'exercice d'imposition 2027 (année de revenus 2026), le montant de 0,15 euro par kilomètre parcouru entre le domicile et le lieu de travail au moyen du propre véhicule ne sera plus déductible à l'impôt des personnes physiques pour les véhicules dont les frais professionnels (déplacements effectués dans l'exercice de l'activité professionnelle) autres que les frais d'électricité et de carburant ne seront pas déductibles à partir de l'exercice d'imposition 2027 conformément à la réglementation générale? Cela signifie-t-il donc, *a contrario*, que le forfait de 0,15 euro par kilomètre parcouru entre le domicile et

andere autokosten dan brandstof en elektriciteit – nog aftrekbaar zijn voor:

(1) koolstofemissievrije voertuigen,

(2) plug-in voertuigen aangeschaft tot en met 2029. Plug-in voertuigen aangekocht, geleased of gehuurd vanaf 2030 komen niet meer in aanmerking voor het kostenforfait van 0,15 euro/km,

(3) voertuigen met uitsluitend een verbrandingsmotor, aangekocht, geleased of gehuurd vóór 1 juli 2023, dus de voertuigen met uitsluitend verbrandingsmotor die onder de *grandfathering*-regeling vallen,

(4) voertuigen met uitsluitend een verbrandingsmotor aangekocht, geleased of gehuurd tussen 1 juli 2023 en 31 december 2025, dus de voertuigen met uitsluitend verbrandingsmotor die onder de “uitdoof”-regeling vallen?

Het kostenforfait van 0,15 euro/km is dan nog maximaal mogelijk tot aanslagjaar 2028 (inkomstenjaar 2027). Met andere woorden: voertuigen met uitsluitend een verbrandingsmotor aangekocht, geleased of gehuurd vanaf 1 januari 2026 komen voor het woon-werkverkeer (naast het werk-werkverkeer) dan niet meer in aanmerking voor aftrek ten belope van 0,15 euro/km. Kan de minister dat bevestigen?

6. *Niet-verrekening van roerende voorheffing inzake DBI-beveks als geen bepaalde bedrijfs-leidersbezoldiging is toegekend*

Dit wetsontwerp voegt een artikel 282/1 toe in het WIB 92.

In het oorspronkelijke wetsontwerp (DOC 56 0963/001) stond: “de minimale bezoldiging bepaald in artikel 215, derde lid, 4^o”. In het wetsontwerp na eerste lezing (DOC 56 0963/020) staat: “de minimale bezoldiging bedoeld in artikel 215, derde lid, 4^o”. Het woord “bepaald” werd dus vervangen door het woord “bedoeld”. Wat is de reden voor die aanpassing?

En werkt ook de vrijstelling voor minimale bedrijfs-leidersbezoldiging in de eerste vier boekjaren vanaf oprichting (artikel 215, lid 3, 4^o, WIB 92) hierdoor? Kunnen kleine startende vennootschappen in de eerste vier boekjaren sinds oprichting de roerende voorheffing op

le lieu de travail ne pourra plus s’appliquer, à partir de l’exercice d’imposition 2027, que s’il s’agit d’un véhicule appartenant à l’une des catégories mentionnées ci-dessous dont les “frais généraux”, c’est-à-dire les frais autres que le carburant et l’électricité, sont encore déductibles:

(1) véhicules neutres en carbone,

(2) véhicules rechargeables achetés jusqu’en 2029 inclus. Les véhicules rechargeables achetés, pris en leasing ou en location à partir de 2030 ne pourront plus bénéficier du forfait de 0,15 euro/km,

(3) véhicules équipés exclusivement d’un moteur à combustion et achetés, pris en leasing ou en location avant le 1^{er} juillet 2023, soit les véhicules équipés exclusivement d’un moteur à combustion qui relèvent du régime de protection des droits acquis (*grandfathering*),

(4) véhicules équipés exclusivement d’un moteur à combustion achetés, pris en leasing ou pris en location entre le 1^{er} juillet 2023 et le 31 décembre 2025, soit les véhicules équipés exclusivement d’un moteur à combustion qui relèvent du régime d’extinction?

Le forfait de 0,15 euro/km restera dès lors d’application jusqu’à l’exercice d’imposition 2028 au plus tard (année de revenus 2027). En d’autres termes, les véhicules équipés exclusivement d’un moteur à combustion achetés, pris en leasing ou pris en location à partir du 1^{er} janvier 2026 ne pourront plus bénéficier d’une déduction de 0,15 euro par kilomètre parcouru. Le ministre pourrait-il confirmer cette analyse?

6. *Non-imputation du précompte mobilier relatif aux SICAV-RDT en l’absence d’octroi d’une rémunération déterminée au dirigeant d’entreprise*

Le projet de loi à l’examen ajoute un article 282/1 au CIR92.

Il est question dans le projet de loi initial (DOC 56 0963/001) de “la rémunération minimale prévue à l’article 215, alinéa 3, 4^o”. Or, le texte adopté à la suite de l’examen en première lecture (DOC 56 0963/020) évoque quant à lui “la rémunération minimale visée à l’article 215, alinéa 3, 4^o”. Le mot “prévue” a donc été remplacé par le mot “visée”. Quel est le motif de cette modification?

Et cela signifie-t-il que l’exonération pour la rémunération minimale allouée au dirigeant d’entreprise s’applique au cours des quatre premiers exercices comptables à partir de la constitution (art. 215, alinéa 3, 4^o, CIR92)? Les sociétés débutantes de petite taille peuvent-elles imputer le précompte mobilier relatif aux SICAV-RDT

DBI-beveks verrekenen, ook als ze geen bezoldiging toekennen?

7. Niet-verrekenbaarheid van ingehouden roerende voorheffing op dividend ontvangen van DBI-bevek indien de bezoldigingsvoorwaarde niet voldaan is

Als een vennootschap niet voldoet aan de bezoldigingsvoorwaarde en een dividend ontvangt uit aandelen in een DBI-bevek, waarvoor de DBI-coëfficiënt bijvoorbeeld 99,5 % bedraagt, klopt het dat deze vennootschap de keuze heeft tussen:

(1) de DBI-af trek toepassen op 99,5 % van het ontvangen dividend, waardoor de ingehouden roerende voorheffing op datzelfde gedeelte niet kan worden verrekend;

of

(2) de DBI-af trek niet toepassen op het ontvangen dividend, zodat de ingehouden roerende voorheffing op het volledige dividend kan worden verrekend?

D. Bijkomende antwoorden van de minister

Als antwoord op de replieken van de heer Lode Vereeck (VB) verwijst de *vice-eersteminister en minister van Financiën en Pensioenen, belast met de Nationale Loterij en de Federale Culturele Instellingen*, de heer Jan Jambon, naar zijn eerdere antwoorden.

Hij benadrukt dat, indien dit wetsontwerp een betere bestrijding van fraude mogelijk maakt, dit een positieve ontwikkeling is en er dus wel degelijk baten zijn.

Daarnaast kondigt hij aan dat er nog andere wetsontwerpen in voorbereiding zijn die gericht zijn op het bestrijden van andere vormen van fraude.

De minister herhaalt vervolgens dat selectie geen controle is en zeker geen beschuldiging.

Het feit dat de tweejaarlijkse saldi van bankrekeningen in het CAP worden opgenomen, dateert van de vorige legislatuur en maakt geen deel uit van het huidige wetsontwerp diverse bepalingen.

Met betrekking tot de minimumdrempels verwijst de minister naar de verantwoording van de vorige regering, waarin werd vastgesteld dat criminele organisaties vaak een groot aantal transacties uitvoeren met relatief kleine bedragen. Een veelheid van rekeningen met een klein

au cours des quatre premiers exercices comptables à partir de leur constitution même si elles n'allouent pas de rémunération?

7. Non-imputabilité du précompte mobilier retenu sur le dividende perçu de la SICAV-RDT si la condition de rémunération n'est pas remplie

Si une société ne remplit pas la condition de rémunération et perçoit un dividende réalisé sur les actions ou parts d'une SICAV-RDT dont le coefficient RDT s'élève par exemple à 99,5 %, est-il exact que cette société a le choix entre:

(1) appliquer la déduction RDT à 99,5 % du dividende perçu, ce qui signifie que l'on ne peut pas imputer le précompte mobilier retenu sur cette même partie;

ou

(2) ne pas appliquer la déduction RDT au dividende perçu afin que le précompte mobilier retenu puisse être imputé sur la totalité du dividende?

D. Réponses complémentaires du ministre

Concernant les répliques de M. Lode Vereeck (VB), M. Jan Jambon, *vice-premier ministre et ministre des Finances et des Pensions, chargé de la Loterie Nationale et des Institutions culturelles fédérales*, renvoie aux réponses qu'il a déjà fournies précédemment.

Il souligne que si le projet de loi à l'examen permet de lutter plus efficacement contre la fraude, il s'agira d'une évolution positive qui aura donc bel et bien des effets bénéfiques.

Le ministre annonce en outre que d'autres projets de loi visant à lutter contre d'autres formes de fraude sont encore en préparation.

Le ministre répète ensuite que la sélection ne s'apparente pas à un contrôle et qu'elle ne doit certainement pas être interprétée comme une accusation.

L'enregistrement des soldes bisannuels des comptes bancaires dans le PCC remonte à la législature précédente et ne fait pas partie du projet de loi portant des dispositions diverses à l'examen.

En ce qui concerne les seuils minimums, le ministre renvoie à la justification avancée par le gouvernement précédent, qui avait constaté que les organisations criminelles effectuaient souvent un grand nombre de transactions portant sur des montants relativement

saldo kan dus een belangrijke parameter zijn. Ook dit is niet nieuw en ligt niet ter discussie.

De minister verduidelijkt verder dat het voorbeeld van “de bomma met de envelop” geen fiscale inbreuk vormt.

Hij wijst erop dat een betere dossierselectie net bijdraagt tot een efficiëntere fraudebestrijding. Er is geen onderscheid tussen grote en kleine fraude; artikel 322 WIB 92 maakt dat onderscheid niet. Bovendien gaat het hier om administratief fiscaal recht en niet om fiscaal strafrecht.

Tot slot herinnert de minister eraan dat hij reeds heeft toegelicht dat er steeds een menselijke tussenkomst is, hoe datamining werkt, wat de functie is van een DAM-fiche, welke modules en stappen worden gebruikt, en wat de verdere plannen met het CAP zijn. Hij heeft hier niets meer aan toe te voegen en verwijst naar zijn eerdere antwoorden.

De minister beantwoordt verder de vragen van de heer Wouter Vermeersch (VB).

1. DBI en groepsbijdrage – Eu dividenden – onmiddellijke inwerkingtreding door arrest Hof van Justitie

De aangehaalde problematiek is een inbreuk op de vrijheid van vestiging en niet op de vrijheid van kapitaal. Het arrest John Cockerill is bijgevolg niet van toepassing op de aangehaalde casus.

2. Belastingkrediet voor aangroei van eigen middelen bij winsten- en batenbehalers in de personenbelasting

De basis waarop het belastingkrediet wordt berekend wijzigt niet met het huidige ontwerp. Het aangekaarte probleem is ook vandaag al van toepassing.

Het voorliggende wetsontwerp verhoogt enkel het belastingkrediet, wat een positieve maatregel is voor de zelfstandigen-natuurlijke personen.

De fiscale waarde van een personenwagen is het beroepsmatig of het afschrijfbaar gedeelte van de aanschaffingsprijs, verminderd met de reeds aanvaarde afschrijvingen. Bij een eenmanszaak wordt dus het privaat gedeelte van de investering niet in rekening genomen.

modestes. Un nombre élevé de comptes présentant un solde modeste peut dès lors constituer un paramètre important. Cet élément n'est pas non plus nouveau et ne fait pas l'objet de discussions.

Le ministre précise en outre que l'exemple de la grand-mère avec sa petite enveloppe ne constitue pas une infraction fiscale.

Il souligne qu'une meilleure sélection des dossiers contribue justement à une lutte plus efficace contre la fraude. Il n'y a pas de distinction entre petite et grosse fraude; l'article 322 du CIR92 ne fait pas cette différence. De plus, il s'agit en l'espèce de droit fiscal administratif et non de droit pénal fiscal.

Enfin, le ministre rappelle qu'il a déjà expliqué qu'il y aura toujours une intervention humaine, comment fonctionne le *data mining*, quelle sera la fonction d'une fiche DAM, quels modules et étapes sont prévus, et quels sont les projets futurs concernant le PCC. Il n'a rien à ajouter à ce sujet et renvoie à ses réponses précédentes.

Le ministre répond ensuite aux questions de M. Wouter Vermeersch (VB).

1. RDT et transfert intra-groupe – dividendes européens – entrée en vigueur immédiate par suite de l'arrêt de la Cour de Justice

La problématique soulevée constitue une atteinte à la liberté d'établissement et non à la libre circulation des capitaux. L'arrêt John Cockerill n'est donc pas applicable au cas évoqué.

2. Crédit d'impôt pour l'accroissement des fonds propres accordé aux attributaires de bénéfices et de profits à l'impôt des personnes physiques

La base de calcul du crédit d'impôt ne change pas dans le projet à l'examen. Le problème soulevé existe déjà actuellement.

Le projet de loi à l'examen ne fait qu'augmenter le crédit d'impôt, ce qui constitue une mesure positive pour les indépendants-personnes physiques.

La valeur fiscale d'une voiture particulière correspond à la partie professionnelle ou amortissable du prix d'achat, diminuée des amortissements déjà admis. Dans le cas d'une entreprise individuelle, la partie privée de l'investissement n'est donc pas prise en compte.

3. Opsplitsing forfaitaire vergoeding voor dienstverplaatsingen

Het wetsontwerp wijzigt niets aan het principe dat brandstofkosten, die inbegrepen zijn in de kilometervergoeding, geacht worden om 30 % te bedragen van het geheel.

Ook aan de wijze waarop die 30 % moet worden verdeeld over de elektriciteitskost en de fossiele brandstofkost wordt niets gewijzigd.

Hier blijft het met andere woorden van belang om die verdeling op een logische en verifieerbare wijze te doen.

4. Opsplitsing voordeel van alle aard

Het voordeel van alle aard voor een personenwagen dient berekend te worden volgens de gekende formule van artikel 36, § 2, WIB 92, op basis van onder meer de cataloguswaarde van het kosteloos ter beschikking gestelde voertuig en van een CO₂-percentage. Dat voordeel van alle aard wordt dan geacht all-inclusive te zijn. Er is geen afzonderlijk voordeel van alle aard te bepalen voor de brandstof- of elektriciteitskost.

Ook hier brengt dit wetsontwerp geen wijzigingen aan aan de wijze waarop het voordeel van alle aard moet worden berekend, met uitzondering dan van de regeling voor de fake hybrides die, desgevallend, werd aangepast aan de nieuwste CO₂-meetmethodes (Euro 6^e-bis).

5. Kostenforfait woon-werkverkeer 0,15 euro/km

De beginselen ter zake zijn reeds vastgelegd in de wet van 25 november 2021 houdende fiscale en sociale vergroening van de mobiliteit. De aftrekbaarheid van de forfaitaire kosten van 0,15 euro per kilometer voor de verplaatsingen tussen de woonplaats en de plaats van tewerkstelling zal vanaf 2026 inderdaad alleen behouden blijven voor voertuigen zonder CO₂-uitstoot.

Die aftrek zal ook van toepassing blijven voor voertuigen met uitstoot die vallen onder een van de overgangsregelingen die de aftrek als beroepskosten gedeeltelijk behouden, zoals opgenomen in artikel 550 WIB 92. Het gaat hier om voertuigen aangekocht, geleased of gehuurd vóór 1 juli 2023 alsook de voertuigen aangekocht, geleased of gehuurd vanaf 1 juli 2023 tot 31 december 2025 zolang de kostenaftrek erop van toepassing is, dat wil zeggen tot en met aanslagjaar 2028.

3. Ventilation de l'indemnité forfaitaire pour les déplacements professionnels

Le projet de loi ne modifie en rien le principe selon lequel les frais de carburant, qui sont inclus dans l'indemnité kilométrique, sont réputés représenter 30 % du total.

La manière dont ces 30 % doivent être ventilés entre le coût de l'électricité et le coût des combustibles fossiles n'est pas non plus modifiée.

En d'autres termes, il reste important de procéder à cette ventilation de manière logique et vérifiable.

4. Ventilation de l'avantage de toute nature

L'avantage de toute nature pour une voiture particulière doit être calculé selon la formule connue de l'article 36, § 2, CIR92, donc sur la base, entre autres, de la valeur catalogue du véhicule mis gratuitement à disposition et d'un pourcentage-CO₂. Il est considéré que cet avantage de toute nature est *all inclusive*. Il n'y a pas d'avantage de toute nature distinct à déterminer pour le coût du carburant ou de l'électricité.

En l'occurrence également, le projet de loi à l'examen n'apporte aucune modification à la manière dont l'avantage de toute nature doit être calculé, à l'exception du régime applicable aux faux hybrides qui, le cas échéant, a été adapté aux dernières méthodes de mesure du CO₂ (Euro 6^e-bis).

5. Forfait de frais de 0,15 euro par kilomètre parcouru entre le domicile et le lieu travail

Les principes en la matière ont déjà été fixés dans la loi du 25 novembre 2021 organisant le verdissement fiscal et social de la mobilité. La déductibilité des frais forfaitaires de 0,15 euro par kilomètre pour les déplacements entre le domicile et le lieu de travail ne sera en effet maintenue à partir de 2026 que pour les véhicules sans émissions de CO₂.

Cette déduction restera également applicable aux véhicules émetteurs de CO₂ relevant de l'un des régimes transitoires qui maintiennent partiellement la déduction en tant que frais professionnels, tels que prévus à l'article 550 du CIR92. Il s'agit en l'occurrence des véhicules achetés, pris en leasing ou en location avant le 1^{er} juillet 2023, ainsi que des véhicules achetés, pris en leasing ou en location entre le 1^{er} juillet 2023 et le 31 décembre 2025, tant que la déduction des frais s'y appliquera, c'est-à-dire jusqu'à l'exercice d'imposition 2028 inclus.

Via dit wetsontwerp zal de 0,15 euro aftrek ook van toepassing blijven op de hybride voertuigen van artikel 66, § 1/1, WIB 92, zoals voorzien in artikel 23 van dit wetsontwerp. Die 0,15 euro aftrek blijft dan wel 0,15 euro, er wordt met andere woorden geen percentage op toegepast.

6. Niet-verrekening van roerende voorheffing inzake DBI-beveks als geen bepaalde bedrijfsleidersbezoldiging is toegekend

De vervanging van het woord “bepaald” door “bedoeld” betreft een legistieke correctie, aangebracht bij het nazicht van de drukproef door de Commissiedienst, om een consequente toepassing van de juiste terminologie te verzekeren.

Artikel 215, derde lid, 4°, WIB 92 dient in zijn geheel in aanmerking te worden genomen, inclusief de eerste vier boekjaren waarvoor er geen minimumbezoldiging vereist is. Kleine startende vennootschappen kunnen dus in de eerste vier boekjaren sinds oprichting de roerende voorheffing op DBI-beveks verrekenen ook als ze geen bezoldiging toekennen.

7. Niet-verrekenbaarheid van ingehouden roerende voorheffing op dividend ontvangen van DBI-bevek indien de bezoldigingsvoorwaarde niet voldaan is

Het toepassingsgebied van artikel 282/1 WIB 92 is inderdaad beperkt tot dividenden die in toepassing van artikel 202 en 203 van de winst worden afgetrokken. Het verrekeningsverbod geldt dus niet voor DBI-dividenden die niet van de winst worden afgetrokken.

E. Bijkomende replieken van de leden en de minister

Voor de heer Lode Vereeck (VB) zijn de antwoorden van de minister zowel verrassend als verontrustend.

Het feit dat datamining gepaard gaat met een menselijke tussenkomst wordt regelmatig opgeworpen als argument. Deze menselijke controle ontbreekt echter in de eerste fase (dossierselectie).

Elke burger heeft recht op een eerlijk proces en een beroepsprocedure, zowel in de fase van de selectie als van de controle. Fiscale experts wijzen erop dat de burger in beide fases moet weten waarom hij geselecteerd is en dat deze selectie niet mag gebeuren door een volledig geautomatiseerd systeem. Om die reden dringt de spreker aan op *counterfactual* verklaringen. Iemand moet de betrokkenen uitleg verschaffen over de reden van selectie. Verschillende commissieleden

Le projet de loi à l'examen prévoit aussi, en son article 23, que la déduction de 0,15 euro continuera également à s'appliquer aux véhicules hybrides visés à l'article 66, § 1^{er}/1, du CIR92. Cette déduction de 0,15 euro restera toutefois de 0,15 euro. En d'autres termes, aucun pourcentage n'y sera appliqué.

6. Non-imputation du précompte mobilier sur les SICAV-RDT en l'absence d'octroi d'une rémunération déterminée au dirigeant d'entreprise

Le remplacement du mot “prévue” par le mot “visée” est une correction d'ordre légistique apportée par le service des commissions lors de la relecture de l'épreuve, en vue d'assurer une application cohérente de la terminologie adéquate.

L'article 215, alinéa 3, 4°, du CIR92 s'appliquera sans restriction, y compris les quatre premiers exercices comptables pour lesquels aucune rémunération minimale n'est requise. Les petites entreprises en phase de démarrage pourront donc, au cours des quatre premiers exercices comptables à partir de leur constitution, imputer le précompte mobilier sur les SICAV-RDT, même si elles n'octroient aucune rémunération.

7. Non-imputabilité du précompte mobilier retenu sur le dividende perçu de la SICAV-RDT si la condition de rémunération n'est pas remplie

Le champ d'application de l'article 282/1 du CIR92 est en effet limité aux dividendes déduits des bénéfices en application des articles 202 et 203. L'interdiction d'imputation ne s'applique donc pas aux dividendes RDT qui ne sont pas déduits des bénéfices.

E. Répliques complémentaires des membres et du ministre

M. Lode Vereeck (VB) juge les réponses du ministre à la fois surprenantes et inquiétantes.

L'argument selon lequel le *data mining* s'accompagnera d'une intervention humaine est régulièrement avancé. Ce contrôle humain sera toutefois absent lors de la première phase (sélection de dossiers).

Chaque citoyen a droit à un procès équitable et à une procédure de recours, tant lors de la sélection que du contrôle. Les experts fiscaux soulignent que, lors de ces deux phases, les citoyens devront être informés des raisons pour lesquelles leur dossier a été sélectionné et savoir que cette sélection ne peut pas être opérée par un système entièrement automatisé. C'est pourquoi l'intervenant insiste sur la nécessité de fournir des explications contrefactuelles. Les personnes

en andere observatoren lijken niet te begrijpen dat er ook in deze eerste fase een menselijke tussenkomst moet plaatsvinden.

De voorliggende plannen zullen uiteindelijk tot juridische problemen leiden.

Verder antwoordde de minister op de vraag naar externe audits dat teams van de FOD Financiën reeds audits uitvoeren. Deze verlopen echter niet extern, waardoor de FOD Financiën zowel rechter als partij is. Een externe toezichthouder is noodzakelijk, eventueel zelfs via een algoritme.

De opleidingen die de minister opsomde leken voorts eerder van technische aard (bijvoorbeeld over datakwantiteitsanalyse) en gaan niet over de sociaalwetenschappelijke problemen in verband met datamining, zoals bias. Kunnen ambtenaren van de FOD Financiën een dergelijk probleem herkennen en er iets aan doen? Het antwoord is volgens de spreker negatief. De lijst met opleidingen zou bijgevolg uitgebreid moeten worden.

Tot slot wijst de heer Vereeck op het verschil tussen een *chilling effect* en een *deterrence effect*. In dat verband kan worden verwezen naar publicaties van de heer Wim Moesen (emeritus hoogleraar, KU Leuven).

De heer Vincent Van Quickenborne (Open Vld) onderhoudt uit de voorgaande replieken dat ook leden van de meerderheid kritische geluiden laten horen over de datamining op het rekeningenregister. Onderhavig debat heeft bijgevolg wel degelijk zin. Het persagentschap *Belga* citeert de heer Mathieu Michel (MR) die verklaarde in de vorige regering reeds sterke bedenkingen te hebben bij het CAP en er nog steeds hetzelfde over te denken. Volgens de spreker zou de heer Michel de voorliggende tekst niet goedkeuren indien hij in alle vrijheid kon stemmen.

De heer Van Quickenborne wenst vervolgens te reageren op een beschuldiging aan zijn adres. Na vijftig uur debat kwam de Vooruit-fractie bij monde van de heer Niels Tas (Vooruit) voor het eerst tussen, al kwam hij weinig verder dan het voorlezen van een debatfiche. Zo werd beweerd dat Open Vld "valsspelers wil laten doen". Tijdens zijn ministerschap heeft de heer Van Quickenborne met alle middelen de strijd tegen ernstige en georganiseerde criminaliteit gevoerd, bijvoorbeeld door middel van multidisciplinaire onderzoeksteams (MOTEM) of door zijn inzet voor een uitleveringsverdrag met de Verenigde Arabische Emiraten. Dit kwam hem zelfs op persoonlijke bedreigingen te staan. Het is daarom onredelijk om te

concernées devront être informées des motifs sous-tendant la sélection de leur dossier. Plusieurs membres et d'autres observateurs ne saisissent visiblement pas la nécessité de prévoir une intervention humaine lors de cette première phase également.

Les mesures envisagées conduiront *in fine* à des problèmes juridiques.

Le ministre a par ailleurs répondu à la question relative aux audits externes en indiquant que des équipes du SPF Finances effectuaient déjà des audits. Ceux-ci n'étant toutefois pas externalisés, le SPF Finances y est à la fois juge et partie. Il est nécessaire de prévoir des audits externes, éventuellement via des algorithmes.

Les formations énumérées par le ministre semblaient plutôt être de nature technique (notamment celle portant sur l'analyse de la qualité de données) et ne traitent pas des problèmes socioscientifiques liés au *data mining*, notamment les biais. Les fonctionnaires du SPF Finances sont-ils en mesure d'identifier ces problèmes et d'y remédier? L'intervenant en doute. La liste des formations devra donc être étendue.

Enfin, M. Vereeck souligne la différence entre la peur de la sanction ou l'effet dissuasif (*chilling effect*) et l'effet de dissuasion (*deterrence effect*). Il renvoie à ce propos aux publications de M. Wim Moesen (professeur émérite à la KU Leuven).

M. Vincent Van Quickenborne (Open Vld) retient des répliques précédentes que même des membres de la majorité émettent des critiques sur l'extension envisagée du PCC au *data mining*. Le débat actuel a donc tout son sens. L'agence de presse *Belga* a rapporté les propos de M. Mathieu Michel (MR), qui avait déjà exprimé son malaise à l'égard du PCC sous la précédente législature et qui n'en pense pas moins aujourd'hui. Selon l'intervenant, M. Michel n'approuverait pas le texte à l'examen s'il pouvait voter en toute liberté.

M. Van Quickenborne souhaite ensuite réagir à une accusation portée à son encontre. Au terme de 50 heures de débat, le groupe Vooruit est intervenu pour la première fois par la voix de M. Niels Tas, même si celui-ci s'est borné à lire une fiche contenant des éléments de langage. Il a ainsi affirmé que l'Open Vld entendait laisser la voie libre aux tricheurs. Au cours de son mandat ministériel, M. Van Quickenborne a pourtant tout mis en œuvre pour lutter contre la criminalité grave et organisée, par exemple en mettant sur pied des équipes d'enquête pluridisciplinaires (MOTEM) ou en s'engageant en faveur d'un traité d'extradition avec les Émirats arabes unis. Cela lui a même valu des menaces personnelles. Il est

beweren dat de fractie van de spreker fraudebestrijding niet ernstig neemt.

Verder werd door Vooruit verwezen naar andere landen, zoals Oostenrijk, waar inderdaad ook een rekeningenregister bestaat. In Oostenrijk wordt echter geen datamining op deze databank toegelaten. De vergelijking slaat dan ook nergens op.

Ten derde sprak de heer Tas over snelheidscontroles in het verkeer. In de media werd zelfs een vergelijking gemaakt tussen “*money control*” en trajectcontroles, wellicht onder druk van N-VA. De vergelijking gaat echter niet op, aangezien trajectcontroles een marge van 6 kilometer per uur hanteren, wat de heer Van Quickenborne als minister steeds heeft gerespecteerd.

Ten slotte antwoordde de heer Tas niet op de vraag waarom datamining niet tot ernstige en georganiseerde fraude wordt beperkt. Volgens de spreker is de verklaring dat de regering met dit systeem elke vorm van fraude wil bestrijden, zelfs als het bijvoorbeeld cadeaus binnen een familie betreft waarvan de herkomst van het geld onbekend is. De minister gaf in zijn antwoorden immers aan dat ook kleine bedragen gecontroleerd worden omdat deze eveneens kunnen wijzen op mogelijke fraude.

De minister wijst erop dat zijn woorden systematisch uit hun context worden getrokken. Zijn eerdere antwoord luidde dat het in fraudezaken een fenomeen is om op veel rekeningen kleine bedragen te zetten. Het is bijgevolg logisch om in het kader van fraudebestrijding met dat fenomeen rekening te houden.

De heer Vincent Van Quickenborne (Open Vld) repliceert dat hij het inderdaad had over kleine bedragen die worden opgespoord. Dit kan vermeden worden door zich te beperken tot de ernstige en georganiseerde fraude. De vraag waarom de minister het domein van “*money control*” niet daartoe begrenst bleef tot nu toe onbeantwoord.

De minister verwijst naar zijn eerdere reeks antwoorden.

De heer Dieter Vanbesien (Ecolo-Groen) onthoudt uit het antwoord van de minister dat er niet zoiets bestaat als kleine en grote fraude. Ofwel houdt men zich aan de regels, ofwel niet. Fraude is fraude.

De heer Vincent Van Quickenborne (Open Vld) concludeert daaruit dat het datamining-mechanisme voor elke vorm van fraude, ook de kleinste bedragen, zal worden

donc déraisonnable d'affirmer que le groupe de l'intervenant ne prend pas au sérieux la lutte contre la fraude.

Le groupe Vooruit a également évoqué d'autres pays, notamment l'Autriche, où il existe effectivement un registre des comptes. L'Autriche n'exploite toutefois pas cette banque de données à des fins de *data mining*. Cette comparaison ne tient donc pas la route.

M. Tas a en outre évoqué les contrôles de vitesse sur la voie publique. Les médias ont même établi une comparaison entre le “*money control*” et les radars tronçons, sans doute sous la pression de la N-VA. Cette comparaison n'est toutefois pas pertinente, puisque les radars tronçons appliquent une marge de tolérance de 6 km/h, une limite que M. Van Quickenborne a toujours respectée en tant que ministre.

Enfin, M. Tas n'a pas répondu à la question de savoir pourquoi le recours au *data mining* ne serait pas limité à la fraude grave et organisée. Selon l'intervenant, ce choix s'explique par la volonté du gouvernement de lutter contre toute forme de fraude, même s'il s'agit, par exemple, de sommes offertes en cadeau dans le cadre familial et dont l'origine est inconnue. Dans ses réponses, le ministre a en effet indiqué que même les petites sommes seraient contrôlées, car celles-ci peuvent aussi indiquer l'existence d'une fraude potentielle.

Le ministre souligne que ses propos sont systématiquement sortis de leur contexte. Il a précédemment répondu à ce sujet que, dans les affaires de fraude, il n'est pas rare que de petites sommes soient déposées sur une multitude de comptes. Il est donc logique de tenir compte de ce phénomène dans le cadre de la lutte contre la fraude.

M. Vincent Van Quickenborne (Open Vld) réplique qu'il faisait effectivement référence à la détection de petites sommes. Cette situation pourrait être évitée en limitant le *money control* à la fraude grave et organisée. On ignore toujours pourquoi le ministre refuse de le limiter à cette finalité.

Le ministre renvoie aux diverses réponses qu'il a apportées précédemment à ce sujet.

M. Dieter Vanbesien (Ecolo-Groen) retient de la réponse du ministre qu'il n'existe en réalité pas de petite ou de grande fraude: soit on respecte les règles, soit on ne les respecte pas. Une fraude est une fraude.

M. Vincent Van Quickenborne (Open Vld) en conclut que le mécanisme du *data mining* sera utilisé pour détecter toute forme de fraude, même si les sommes

gebruikt. Hij geeft het voorbeeld van een grootmoeder die haar kleinkinderen een envelop met geld toestopt.

De voorzitter dringt erop aan om geen losstaande zinsneden uit de context te halen en andere sprekers woorden in de mond te leggen. Het door de heer Van Quickenborne aangehaalde voorbeeld werd op geen enkel moment als fraude bestempeld.

De heer Dieter Vanbesien (Ecolo-Groen) betreurt de sfeerschepping die ertoe bijdraagt dat het draagvlak voor fraudebestrijding kan afbrokkelen. De heer Van Quickenborne verkondigt bewust onjuistheden. Zijn voorbeeld van een grootmoeder die geld cadeau doet aan familieleden is hoegenaamd niet als fraude te categoriseren. Mensen worden fout geïnformeerd en vervolgens beweert men dat er geen draagvlak is. Dit getuigt van slechte wil.

De heer Vincent Van Quickenborne (Open Vld) stelt vast dat 79 % van de bevolking zich in een televisiepeiling tegen “*money control*” kantte, nog voor het bovenstaande voorbeeld zelfs maar aan bod was gekomen. Er is inderdaad een gebrek aan draagvlak.

Ten tweede werd verwezen naar de uitspraak van de minister dat er geen onderscheid bestaat tussen grote en kleine fraude. In het koninklijk besluit van 9 februari 2020 tot uitvoering van artikel 29, § 4, van het Wetboek van Strafvordering, wordt echter wel degelijk een definitie van ernstige en georganiseerde fraude geformuleerd. Het is onbegrijpelijk dat de regering zich daar niet toe beperkt. Uit deze keuze volgt dat elke vorm van fraude, zelfs voor zeer lage bedragen, zal kunnen worden vervolgd.

Het lid gaat vervolgens in op een onbeantwoorde vraag. De tweede alinea van de door amendement nr. 16 (DOC 56 0963/005) ingevoegde § 3 is een exacte kopie van een tekst die reeds is opgenomen in het bestaande artikel 5 van de wet van 3 augustus 2012 houdende bepalingen betreffende de verwerking van persoonsgegevens door de Federale Overheidsdienst Financiën in het kader van zijn opdrachten. Beseft de minister dat de in amendement nr. 16 voorgestelde wetgeving getuigt van amateurisme? Een dergelijke improvisatie is onbegrijpelijk voor zo'n ernstig onderwerp.

De laatste onbeantwoorde vraag gaat over de mening van de minister aangaande de opmerkingen van mevrouw Nadia Sminate (N-VA), lid van het Vlaams Parlement, over de voorliggende maatregel.

concernées sont minimales. Il cite l'exemple d'une grand-mère qui donne une enveloppe contenant de l'argent à ses petits-enfants.

Le président insiste pour que les membres ne sortent pas des phrases isolées de leur contexte et qu'ils ne prêtent pas à tort des propos à d'autres intervenants. L'exemple cité par M. Van Quickenborne n'a à aucun moment été qualifié de fraude.

M. Dieter Vanbesien (Ecolo-Groen) déplore le climat négatif actuel qui risque de saper le soutien apporté à la lutte contre la fraude. M. Van Quickenborne répand délibérément des inepties. L'exemple qu'il a cité, à savoir celui d'une grand-mère qui offre de l'argent en cadeau à des membres de sa famille, ne peut en aucun cas être taxé de fraude. Des propos de cette nature font que les citoyens sont mal informés, et d'aucuns prétendent ensuite que le projet de *money control* ne suscite pas l'adhésion. Cela témoigne d'une mauvaise volonté.

M. Vincent Van Quickenborne (Open Vld) constate que, lors d'un sondage télévisé, 79 % des personnes interrogées se sont prononcées contre le *money control*, avant même que l'exemple précité soit connu. Ce projet n'est en effet pas soutenu par la population.

En deuxième lieu, il a été dit que le ministre avait déclaré qu'il n'y avait pas de distinction entre les petites et les grandes fraudes. Or, l'arrêté royal du 9 février 2020 portant exécution de l'article 29, § 4, du Code d'instruction criminelle contient une définition de la fraude sérieuse et organisée. Il est incompréhensible que le gouvernement ne se limite pas à celle-là, ce qui aura pour conséquence que toute forme de fraude, même pour des montants très faibles, pourra faire l'objet de poursuites.

Le membre évoque ensuite une question restée sans réponse. Le § 3, alinéa 2, inséré par l'amendement n° 16 (DOC 56 0963/005), reproduit littéralement un passage de l'article 5 actuel de la loi du 3 août 2012 portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions. Le ministre est-il conscient que la disposition proposée par l'amendement n° 16 témoigne d'un certain amateurisme? Selon l'intervenant, ce degré d'improvisation est incompréhensible pour un sujet aussi sérieux.

La dernière question restée sans réponse porte sur l'opinion du ministre concernant les observations formulées par Mme Nadia Sminate (N-VA), membre du Parlement flamand, au sujet de la mesure à l'examen.

De minister herhaalt dat ieder Parlements­lid vrijheid van meningsuiting heeft. De beslissingen worden door het Parlement genomen.

De heer Vincent Van Quickenborne (Open Vld) concludeert dat er met de opmerkingen van mevrouw Sminate geen rekening wordt gehouden.

De minister benadrukt dat elk Parlements­lid zich over dit onderwerp mag uitspreken en dat het Parlement finaal de beslissing neemt.

De heer Vincent Van Quickenborne (Open Vld) interpreteert dit als een meningsverschil tussen de minister en mevrouw Sminate. Het bewijst dat de N-VA op dit punt verdeeld is, wat de spreker niet verwondert. Volgens hem denken veel N-VA-Parlementsleden er hetzelfde over als mevrouw Sminate, maar worden zij de mond gesnoerd.

De eerder technische antwoorden van de minister blijven in gebreke wat de essentie van de zaak betreft, namelijk het vermoeden van onschuld alsook de privacy van 11 miljoen Belgen die worden ondergraven.

Het lid gaat ervan uit dat de minister van Financiën deze maatregelen niet uit eigen overtuiging doorvoert, maar op aansturen van de Vlaamse socialist.

De heer Wouter Vermeersch (VB) bedankt de minister voor de uitvoerige antwoorden op zijn technische vragen. Eventuele opmerkingen over deze punten zullen in de plenaire vergadering geformuleerd worden.

III. — ARTIKELSGEWIJZE BESPREKING

TITEL I

Algemene bepaling

Artikel 1

Dit artikel regelt de grondwettelijke grondslag van het wetsontwerp en geeft geen aanleiding tot opmerkingen.

Le ministre rappelle que chaque parlementaire jouit de la liberté d'expression. Les décisions sont prises par le Parlement.

M. Vincent Van Quickenborne (Open Vld) en déduit que les observations de Mme Sminate n'ont pas été prises en compte.

Le ministre souligne que tout parlementaire peut se prononcer à ce sujet mais que la décision finale appartient au Parlement.

M. Vincent Van Quickenborne (Open Vld) voit dans cet échange l'expression d'une divergence d'opinions entre le ministre et Mme Sminate. Selon l'intervenant, cela prouve que la N-VA est divisée à ce sujet, ce qui ne l'étonne pas. Selon lui, de nombreux parlementaires de la N-VA partagent l'avis de Mme Sminate, mais sont muselés.

Les réponses plutôt techniques du ministre ne répondent pas aux questions essentielles concernant les atteintes graves portées à la présomption d'innocence et à la protection de la vie privée de onze millions de Belges.

L'intervenant présume que le ministre des Finances ne propose pas ces mesures par conviction personnelle, mais plutôt sous la pression des socialistes flamands.

M. Wouter Vermeersch (VB) remercie le ministre pour ses réponses détaillées à ses questions techniques. Les éventuelles observations sur ces points seront formulées en séance plénière.

III. — DISCUSSION DES ARTICLES

TITRE I^{ER}

Disposition générale

Article 1^{er}

Cet article fixe le fondement constitutionnel du projet de loi et ne donne lieu à aucune observation.

TITEL 2

Financiën

HOOFDSTUK 1

Wijzigingen betreffende de inkomstenbelastingen**Afdeling 1***Vastgoedfiscaliteit*

Artikelen 2 tot 10

Er worden geen opmerkingen geformuleerd bij deze artikelen.

Art. 11

De heren Vereeck en Vermeersch dienen amendement nr. 102 (partim) (DOC 56 0963/028) in, dat ertoe strekt in de punten 1° en 2° de woorden “tot en met aanslagjaar 2025” te vervangen.

De heer Lode Vereeck (VB) verduidelijkt dat het amendement een overgangsmaatregel beoogt te voorzien voor lopende kredietovereenkomsten ter verwerving of behoud van een onroerend goed waarop het fiscaal voordeel reeds van toepassing was.

Voor de toelichting kan worden verwezen naar de verantwoording.

Art. 12

Dit artikel geeft geen aanleiding tot opmerkingen.

Art. 13

De heren Vereeck en Vermeersch dienen amendement nr. 102 (partim) (DOC 56 0963/028) in, dat ertoe strekt in punt 1° de woorden “tot en met aanslagjaar 2025” te vervangen alsook in punt 2° de woorden “zoals het tot en met aanslagjaar 2025 van toepassing is” te vervangen.

Voor de toelichting kan worden verwezen naar artikel 11 en naar de verantwoording.

TITRE 2

*Finances*CHAPITRE 1^{ER}**Modifications relatives aux impôts sur les revenus****Section 1^{re}***Fiscalité immobilière*

Articles 2 à 10

Ces articles ne donnent lieu à aucune observation.

Art. 11

MM. Vereeck et Vermeersch présentent l'amendement n° 102 (partim) (DOC 56 0963/028) tendant à remplacer les mots “jusqu'à l'exercice d'imposition 2025” aux points 1° et 2°.

M. Lode Vereeck (VB) précise que l'amendement à l'examen vise à prévoir une mesure transitoire pour les contrats de crédit en cours conclus en vue de l'acquisition ou de la conservation d'un bien immobilier auquel l'avantage fiscal s'appliquait déjà.

Pour plus de précisions, il est renvoyé à la justification.

Art. 12

Cet article ne donne lieu à aucune observation.

Art. 13

MM. Vereeck et Vermeersch présentent l'amendement n° 102 (partim) (DOC 56 0963/028), tendant à remplacer les mots “jusqu'à l'exercice d'imposition 2025” au point 1°, ainsi que les mots “tel qu'il est applicable jusqu'à l'exercice d'imposition 2025” au point 2°.

Pour les explications, on se reportera à l'article 11 et à la justification.

Art. 14

De heer Van Quickenborne en mevrouw Bertrand dienen amendement nr. 91 (DOC 56 0963/028) in, dat ertoe strekt het eerste lid van dit artikel te vervangen. Voor de toelichting kan worden verwezen naar de verantwoording.

De heer Vincent Van Quickenborne (Open Vld) vult aan dat mensen met een tweede verblijf de interessen van een lopend hypotheckair krediet ten gevolge van deze “woontaks” niet langer fiscaal zullen kunnen aftrekken. De maatregel treft 500.000 mensen en brengt dan ook heel wat ontevredenheid teweeg. 80 % van dit soort contracten zijn overigens in Vlaanderen afgesloten.

Een mogelijk gevolg is dat de huidige huurprijs voor een verhuurder niet meer overeenkomt met zijn financiële planning, aangezien hij geen interessen meer in mindering kan brengen. De “woontaks” zal ertoe leiden dat huurprijzen verder stijgen op een markt die reeds onder druk staat bij gebrek aan aanbod.

De afschaffing van de belastingaftrek is tevens van toepassing op lopende contracten. De spreker stelt voor om het voorbeeld van de hervorming van de woonbonus in Vlaanderen te volgen, waar de engagementen voor lopende contracten door de overheid werden gerespecteerd. Om contractbreuk te vermijden dient de regering enkel toekomstige contracten te viseren.

Afdeling 2

*Ingekomen belastingplichtigen en
ingekomen onderzoekers*

Art. 15

De heren Vereeck en Vermeersch dienen amendement nr. 103 (partim) (DOC 56 0963/028) in, dat ertoe strekt de punten 2°, 3° en 4° te vervangen.

Het amendement beoogt de ongelijke behandeling van ingekomen en binnenlandse belastingplichtigen op het vlak van kosten eigen aan de werkgever weg te nemen. Voor de toelichting kan worden verwezen naar de verantwoording.

Art. 16

De heren Vereeck en Vermeersch dienen amendement nr. 103 (partim) (DOC 56 0963/028) in, dat ertoe strekt de punten 1°, 2° en 3° te vervangen.

Art. 14

M. Van Quickenborne et Mme Bertrand présentent l'amendement n° 91 (DOC 56 0963/028), tendant à remplacer l'alinéa 1^{er} de cet article. Pour les explications, on se reportera à la justification.

M. Vincent Van Quickenborne (Open Vld) ajoute que les personnes disposant d'une seconde résidence ne pourront plus déduire fiscalement les intérêts d'un crédit hypothécaire en cours en raison de cette “taxe sur le logement”. La mesure affectera 500.000 personnes et suscite dès lors beaucoup de mécontentement. 80 % des contrats de ce type sont d'ailleurs conclus en Flandre.

Une conséquence possible est que le loyer demandé actuellement par un bailleur ne correspondra plus à sa planification financière, puisqu'il ne pourra plus déduire les intérêts. Cette “taxe sur le logement” entraînera une nouvelle hausse des loyers sur un marché qui est déjà sous pression en raison de l'offre insuffisante.

La suppression de la déduction fiscale s'appliquera également aux contrats en cours. L'intervenant propose de suivre l'exemple de la réforme du bonus logement en Flandre, où les engagements relatifs aux contrats en cours ont été respectés par les autorités. Pour éviter une rupture de contrat, le gouvernement doit viser uniquement les contrats futurs.

Section 2

*Contribuables impatriés et
chercheurs impatriés*

Art. 15

MM. Vereeck et Vermeersch présentent l'amendement n° 103 (partim) (DOC 56 0963/028), tendant à remplacer le 2°, le 3° et le 4°.

L'amendement vise à supprimer l'inégalité de traitement entre les contribuables impatriés et les contribuables résidents en matière de frais propres à l'employeur. Pour les explications, on se reportera à la justification.

Art. 16

MM. Vereeck et Vermeersch présentent l'amendement n° 103 (partim) (DOC 56 0963/028), tendant à remplacer le 2°, le 3° et le 4°.

Voor de toelichting kan worden verwezen naar artikel 15 en naar de verantwoording.

Artikelen 16/1 (*nieuw*) en 17

Deze artikelen geven geen aanleiding tot opmerkingen.

Afdeling 3

Flexi-jobs

Artikelen 18 en 19

Deze artikelen geven geen aanleiding tot opmerkingen.

Artikelen 19/1 tot 19/9 (*nieuw*)

De heer Van Quickenborne en mevrouw Bertrand dienen amendement nr. 92 (DOC 56 0963/028) in, dat ertoe strekt de artikelen 19/1 tot 19/9 (*nieuw*) in te voeren. Voor nadere toelichting bij deze artikelen kan worden verwezen naar de verantwoording.

De heer Vincent Van Quickenborne (Open Vld) verduidelijkt dat het amendement beoogt flexi-jobs uit te breiden naar alle sectoren, rekening houdend met de modaliteiten voorzien in het regeerakkoord.

De regering wil het fiscaal vrijgestelde plafond voor flexi-jobs optrekken van 12.000 euro naar 18.000 euro met indexering. De spreker steunt deze verhoging, al voegt hij eraan toe dat de N-VA-fractie tijdens de vorige legislatuur nochtans hevig heeft gefulmineerd tegen de invoering van een dergelijk plafond. Een opheffing door de huidige regering zit er kennelijk niet in.

De kritiek inzake staatssteun werd door de minister afdoende beantwoord. Indien het Europees intracommunautair handelsverkeer verstoord wordt, zou er sprake kunnen zijn van problematische staatssteun. Het voordeel van een flexi-job komt echter terecht bij individuele werknemers, waardoor het probleem niet aan de orde is.

Daarnaast merkten sommige observatoren op dat de Raad van State kanttekeningen plaatst bij de uitbreiding van flexi-jobs naar alle sectoren. Deze kritiek houdt geen steek, aangezien de Raad van State op dit punt nog geen advies heeft uitgebracht.

De spreker wenst het wetsontwerp robuuster te maken door de veralgemening voor alle sectoren daadwerkelijk

Pour les explications, on se reportera à l'article 15 et à la justification.

Articles 16/1 (*nouveau*) et 17

Ces articles ne donnent lieu à aucune observation.

Section 3

Flexi-jobs

Articles 18 et 19

Ces articles ne donnent lieu à aucune observation.

Articles 19/1 à 19/9 (*nouveaux*)

M. Van Quickenborne et Mme Bertrand présentent l'amendement n° 92 (DOC 56 0963/028), tendant à insérer les articles 19/1 à 19/9 (*nouveaux*). Pour davantage d'explications sur ces articles, on se reportera à la justification.

M. Vincent Van Quickenborne (Open Vld) précise que l'amendement vise à étendre les flexi-jobs à tous les secteurs, en tenant compte des modalités prévues dans l'accord de gouvernement.

Le gouvernement souhaite relever le plafond fiscalement exonéré pour les flexi-jobs de 12.000 euros à 18.000 euros, avec indexation. L'intervenant soutient cette mesure, tout en ajoutant que le groupe N-VA avait pourtant vivement protesté contre l'instauration d'un tel plafond sous la législature précédente. Une suppression du plafond par le gouvernement actuel n'est manifestement pas envisagée.

Le ministre a bien répondu aux critiques relatives au respect des règles en matière d'aides d'État. Si les échanges commerciaux intracommunautaires européens étaient perturbés, il pourrait être question d'une aide d'État problématique. L'avantage d'un flexi-job bénéficie toutefois à des travailleurs individuels, de sorte que le problème ne se pose pas.

En outre, certains observateurs ont prétendu que le Conseil d'État avait émis des réserves quant à l'extension des flexi-jobs à tous les secteurs. Cette critique est infondée, puisque le Conseil d'État n'a pas encore rendu d'avis sur ce point.

L'intervenant souhaite rendre le projet de loi plus robuste en généralisant effectivement son application

in te voeren. In het regeerakkoord werd deze uitbreiding immers beloofd vanaf 1 januari 2026. Door het uitstelgedrag van de regering wordt die belofte niet nagekomen.

Het artikel 19/2 (*nieuw*) vervangt artikel 2 van de wet van 16 november 2015 houdende diverse bepalingen inzake sociale zaken. De voornoemde wet wordt daardoor van toepassing op alle werknemers en sectoren, behalve voor bepaalde uitzonderingen die de sociale partners, of de bevoegde ministers in het geval van de overheidssector, kunnen overeenkomen. Voor de kinderopvang zouden specifieke regels gelden en voor de artistieke sector geldt een uitsluiting.

Artikel 19/3 (*nieuw*) wijzigt artikel 4 van de voornoemde wet van 16 november 2015 en beoogt enkele aanpassingen om de wettekst coherenter te maken. Er worden bepalingen voorzien die tot meer flexibiliteit leiden. Werknemers mogen momenteel geen vast contract hebben in een onderneming en tegelijk met een flexi-job actief zijn in een verbonden onderneming. De heer Van Quickenborne wil deze voorwaarde wijzigen voor uitzendkrachten. Een ander voorstel is om wie voltijds werkt wel toe te laten een flexi-job binnen een verbonden onderneming uit te oefenen. Ten slotte is het de bedoeling de regelgeving voor gepensioneerden te versoepelen: in plaats van na twee kwartalen zou er meteen na de pensionering in een flexi-job ingestapt kunnen worden.

Artikel 19/4 (*nieuw*) komt tegemoet aan een vraag van de horecasector om een uurloon van maximaal 21 euro te hanteren in plaats van een minimumloon.

In artikel 19/5 (*nieuw*) wordt voorgesteld om een systeem van elektronische aangifte en doorgifte mogelijk te maken. Het bestaande papieren proces dient te worden gemoderniseerd.

Artikelen 19/6 en 19/7 (*nieuw*) betreffen technische aanpassingen.

Artikel 19/8 (*nieuw*) voorziet voor het jaar 2026 de mogelijkheid tot een gehele of gedeeltelijke uitsluiting of toelating van sectoren op kwartaalbasis.

Artikel 19/9 (*nieuw*) geeft de Ministerraad ten slotte de bevoegdheid om gedeeltelijke toelatingen om te vormen tot gedeeltelijke uitsluitingen van het toepassingsgebied, alsook om gehele of gedeeltelijke uitsluitingen te behouden.

à tous les secteurs. En effet, l'accord de gouvernement promettait cette extension à partir du 1^{er} janvier 2026. À force de reporter sans cesse, le gouvernement n'a toutefois pas tenu cette promesse.

L'article 19/2 (*nouveau*) remplacera l'article 2 de la loi du 16 novembre 2015 portant des dispositions diverses en matière sociale. En conséquence, la loi précitée s'appliquera à tous les travailleurs et à tous les secteurs, à quelques exceptions près qui pourront être convenues entre les partenaires sociaux, ou les ministres compétents dans le cas du secteur public. Des règles spécifiques s'appliqueront à la garde d'enfants et le secteur artistique sera exclu des flexi-jobs.

L'article 19/3 (*nouveau*) modifie l'article 4 de la loi précitée du 16 novembre 2015 et vise à apporter quelques modifications destinées à rendre le texte de loi plus cohérent. Des dispositions sont prévues pour accroître la flexibilité. Aujourd'hui, les travailleurs ne peuvent pas être liés par un contrat fixe dans une entreprise et exercer simultanément un flexi-job dans une entreprise liée. M. Van Quickenborne souhaite modifier cette condition pour les travailleurs intérimaires. Une autre proposition consiste à autoriser les travailleurs à temps plein à exercer un flexi-job dans une entreprise liée. Enfin, l'objectif est d'assouplir la réglementation applicable aux retraités: ces derniers pourraient exercer un flexi-job immédiatement après le départ à la retraite, au lieu de devoir attendre deux trimestres.

L'article 19/4 (*nouveau*) répond à une demande du secteur horeca visant à appliquer un salaire horaire de 21 euros au maximum au lieu d'un salaire minimum.

L'article 19/5 (*nouveau*) propose de mettre en place un système électronique qui enregistre et met à jour la déclaration. Le processus papier actuel doit être modernisé.

Les articles 19/6 et 19/7 (*nouveaux*) concernent des modifications techniques.

L'article 19/8 (*nouveau*) prévoit, pour l'année 2026, la possibilité d'exclure ou d'autoriser totalement ou partiellement certains secteurs sur une base trimestrielle.

Enfin, l'article 19/9 (*nouveau*) habilite le Conseil des ministres à transformer des autorisations partielles en exclusions partielles du champ d'application et à maintenir des exclusions totales ou partielles.

Art. 20

Het door *de heer Van Quickenborne* en *mevrouw Bertrand* ingediende *amendement nr. 93* (DOC 56 0963/028) wordt ingetrokken.

De heer Vincent Van Quickenborne (Open Vld) stipt aan dat de minister in zijn antwoorden een duidelijke uiteenzetting gaf over het aanslagjaar “speciaal” en de mogelijke effecten. De minister heeft afdoende geantwoord op de opmerking van de Raad van State dienaangaande.

Afdeling 4

Autofiscaliteit

Artikelen 21 tot 27

Deze artikelen geven geen aanleiding tot opmerkingen.

Art. 27/1 (*nieuw*)

De heer Van Quickenborne en *mevrouw Bertrand* dienen *amendement nr. 94* (DOC 56 0963/028) in, dat ertoe strekt een artikel 27/1 (*nieuw*) in te voeren. Voor de toelichting kan worden verwezen naar de verantwoording.

De heer Vincent Van Quickenborne (Open Vld) voegt daaraan toe dat het amendement nr. 94 een oplossing voorziet voor kopers van hybride voertuigen die door de regering op het verkeerde been werden gezet op het vlak van fiscaliteit.

Tijdens de algemene bespreking verklaarde de minister in zijn antwoorden dat het tijd is voor stabiliteit. De verguisde Vivaldi-regering zorgde nochtans voor de elektrificatie van bedrijfswagens en lanceerde daarmee het meest succesvolle systeem in Europa. De Europese Commissie verklaarde dat elk land het voorbeeld van het pionierende België zou moeten volgen. De regeling was bovendien stabiel, aangezien deze enkel van toepassing was op wagens die in de toekomst werden aangeschaft. Er was geen sprake van contractbreuk voor lopende contracten.

In het regeerakkoord werd plotseling een stap achteruit gezet door een uitzonderingssysteem voor hybride wagens voor te spiegelen. De voorziene uitdoving van de fiscale aftrek zou teruggedraaid worden. Nadat tal van vennootschappen reeds bestellingen hadden geplaatst, moest de minister op 27 juni 2025 zijn belofte terugkomen.

Art. 20

L'*amendement n° 93* (DOC 56 0963/028) présenté par *M. Van Quickenborne* et *Mme Bertrand* est retiré.

M. Vincent Van Quickenborne (Open Vld) souligne qu'au cours de ses réponses, le ministre a donné des explications claires sur l'exercice d'imposition “spécial” et sur ses effets potentiels. Le ministre a répondu de manière satisfaisante à l'observation du Conseil d'État à ce sujet.

Section 4

Fiscalité automobile

Art. 21 à 27

Ces articles ne donnent lieu à aucune observation.

Art. 27/1 (*nouveau*)

M. Van Quickenborne et *Mme Bertrand* présentent l'*amendement n° 94* (DOC 56 0963/028) tendant à insérer un article 27/1 (*nouveau*). Pour plus de précisions, il est renvoyé à la justification.

M. Vincent Van Quickenborne (Open Vld) ajoute que l'*amendement n° 94* prévoit une solution pour les acheteurs de véhicules hybrides qui ont été induits en erreur par le gouvernement en matière de fiscalité.

Au cours de la discussion générale, le ministre a répondu que l'heure était à la stabilité. Le gouvernement Vivaldi a été critiqué, mais il a pourtant induit l'électrification des voitures de société, et ainsi lancé le système le plus performant d'Europe. La Commission européenne a déclaré que les autres pays devraient suivre l'exemple pionnier de la Belgique. Ce régime était en outre stable, puisqu'il ne devait s'appliquer qu'aux futures voitures devant être achetées. Il n'y a eu aucune rupture de contrat pour les contrats en cours.

L'accord de gouvernement a brusquement fait marche arrière en faisant miroiter un système d'exception pour les voitures hybrides. L'extinction prévue de la déduction fiscale devait être annulée. Après que de nombreuses entreprises avaient déjà passé commande, le ministre a dû revenir sur sa promesse le 27 juin 2025.

Het amendement beoogt de beperkte groep die tussen 31 januari 2025 en 27 juni 2025 een (plug-in) hybride bestelde alsnog te laten genieten van de in het regeerakkoord voorziene regeling.

De voorwaarden van de *Recovery and Resilience Facility* blijven met deze overgangsregeling gerespecteerd.

Afdeling 5

Investeringsaftrek

Art. 28 tot 31

Over deze artikelen worden geen opmerkingen gemaakt.

Afdeling 6

Onderhoudsuitkeringen

Art. 32 tot 35

De heer François De Smet (DéFI) dient amendement nr. 61/partim (DOC 56 0963/01) in, tot weglating van artikel 32 van dit wetsontwerp.

De artikelen 32 tot 35 van het wetsontwerp houdende diverse bepalingen strekken tot vermindering van de aftrekbaarheid van de onderhoudsuitkeringen. De huidige 80 % wordt teruggebracht tot 70 % voor uitkeringen die tussen 1 januari 2025 en 31 december 2025 worden betaald, tot 60 % bij uitkeringen betaald tussen 1 januari 2026 en 31 december 2026, en tot 50 % bij uitkeringen betaald vanaf 1 januari 2027. Als ratio legis van deze bepalingen, net als van andere bepalingen in het fiscale deel van het wetsontwerp, wordt de sanering van de overheidsfinanciën aangevoerd; de regering verantwoordt dit op grond van het feit dat samenwonende ouders in dezen worden benadeeld ten opzichte van uit de echt gescheiden ouders. Thans mag een gescheiden ouder die onderhoudsgeld moet betalen voor een kind van een ex-echtgeno(o)t(e) de belastbare basis verlagen door 80 % van de daadwerkelijk betaalde bedragen af te trekken. Die regeling biedt een aanzienlijk belastingvoordeel en is een stimulans voor schuldenaren om het onderhoudsgeld daadwerkelijk en regelmatig te betalen. Toch blijft het aan kinderen verschuldigde onderhoudsgeld in maar liefst 47 % van de gevallen onbetaald. De andere ouder (degene die het onderhoudsgeld moet ontvangen) kan daarentegen niets aftrekken, maar krijgt wel een ander voordeel, namelijk de verhoging van de belastingvrije som voor een kind

L'objectif de l'amendement à l'examen est de permettre au petit nombre de personnes ayant commandé un véhicule hybride (rechargeable) entre le 31 janvier et le 27 juin 2025 de néanmoins bénéficier du régime prévu par l'accord de gouvernement.

Ce régime transitoire ne portera pas atteinte aux conditions de la Facilité pour la reprise et la résilience.

Section 5

Déduction pour investissement

Art. 28 à 31

Les articles 28 à 31 ne font l'objet d'aucune discussion.

Section 6

Rentes alimentaires

Art. 32 à 35

M. François De Smet (DéFI) présente l'amendement n° 61/partim (DOC 56 0963/021) tendant à supprimer l'article 32 du présent projet de loi.

Les articles 32 à 35 du projet de loi portant dispositions diverses mettent en œuvre une réduction de la déductibilité des rentes alimentaires: – de 80 % à 70 % pour les rentes payées entre le 1^{er} janvier 2025 et le 31 décembre 2025; – à 60 % pour les rentes payées entre le 1^{er} janvier 2026 et le 31 décembre 2026; – à 50 % pour celles à partir du 1^{er} janvier 2027. La *ratio legis* de ces dispositions, à l'instar d'autres du volet fiscal dudit projet de loi, vise l'assainissement des finances publiques et le gouvernement avance comme justification que les parents cohabitants sont moins bien lotis que les parents divorcés à cet égard. Actuellement, un parent séparé qui doit verser une pension alimentaire pour un enfant ou un époux peut diminuer sa base imposable en déduisant 80 % des sommes effectivement versées. Ce mécanisme constitue un avantage fiscal significatif et un incitant pour que le débiteur paie effectivement et régulièrement les pensions alimentaires. Cependant, les pensions alimentaires dues aux enfants restent impayées dans pas moins de 47 % des cas. L'autre parent (celui qui doit recevoir la pension alimentaire) ne peut, quant à lui, rien déduire mais bénéficie d'un autre avantage; la majoration de la quotité exemptée d'impôt pour enfant à charge. Cette situation crée un déséquilibre car l'avantage fiscal pour enfant à charge est un montant fixe et limité, tandis que les 80 % de

ten laste. Die situatie schept een onbalans omdat het belastingvoordeel voor een kind ten laste een vast en beperkt bedrag is, terwijl de 80 % van het onderhoudsgeld aftrekbaar is zonder bovengrens. De beide gescheiden ouders worden dus niet gelijk behandeld. Door de aftrekbaarheid te verlagen van 80 % naar 50 % verliest de schuldenaar 30 % van de belastingaftrek wanneer de maatregelen volledig zullen worden toegepast op de inkomsten vanaf 2027. Bovendien is het niet zeker dat de Arizonaregering die nieuwe middelen zal investeren in de DAVO, de overheidsdienst die voorschotten betaalt en onderhoudsgeld invordert. Daarenboven is de vermindering van de aftrekbaarheid volgens vergelijkbare voorwaarden discriminerend voor de ouders van wie het kind buiten de Europese Economische Ruimte woont. Deze maatregel leidt immers tot een ongelijke behandeling tussen de ouders naargelang van de woonplaats van hun kind, aangezien het niet te rechtvaardigen valt dat de financiële bijdrage tot de opvoeding en het welzijn fiscaal wordt erkend voor een kind dat in de Europese Economische Ruimte woont, maar niet voor een kind dat elders in de wereld woont. Voorts heeft deze maatregel vooral gevolgen voor gezinnen met een migratieachtergrond, aangezien die statistisch gezien meer kans hebben om kinderen te hebben die buiten de EER wonen. Het beginsel van gelijkheid inzake belastingen houdt echter in dat de belastingplichtigen die zich in een vergelijkbare situatie bevinden (in dit geval gescheiden ouders die onderhoudsgeld betalen) gelijk moeten worden behandeld, ongeacht het land waar hun kind woont. Bijgevolg strekt dit amendement ertoe die discriminerende bepalingen weg te laten.

De heer Lode Vereeck en de heer Wouter Vermeersch (VB) dienen amendement nr. 104/partim (DOC 56 0963/028) in, tot weglating van artikel 32 van het wetsontwerp.

Die indieners zien deze maatregel als asociaal, onrechtvaardig en inefficiënt. De verlaging van de aftrekbaarheid van onderhoudsuitkeringen van 80 % naar 70 %, 60 % en dan 50 % betekent een lager beschikbaar inkomen voor de alimentatiebetaler en zijn eventueel nieuw samengesteld gezin. Een aanzienlijk aantal van de in kracht van gewijsde gegane rechterlijke uitspraken over onderhoudsuitkeringen zal op korte termijn moeten worden herzien om het bedrag van de onderhoudsuitkeringen dat momenteel wordt betaald of toegekend, aan te passen aan de hier besproken bepalingen. Dat zal leiden tot de juridisering van familiale afspraken en nieuwe conflicten tussen de ouders, waarvan de kinderen de dupe zullen zijn. Er dreigt bovendien grote rechtsonzekerheid te ontstaan door de overbelasting van het gerecht. Vandaag bedragen de wachttijden bij de familierechtbanken al zes tot negen jaar.

pension alimentaire sont déductibles sans plafond. Les deux parents séparés ne sont donc pas traités sur un même pied d'égalité. En diminuant la déductibilité de 80 à 50 %, le débiteur perdra 30 % de déduction fiscale lorsque les mesures seront pleinement appliquées pour les revenus 2027 et ultérieurs. Il n'est par ailleurs pas avéré que le gouvernement Arizona investira ces nouveaux moyens dans le SECAL, le service public qui paie des avances et récupère les pensions alimentaires. Par ailleurs, la réduction de la déductibilité selon des modalités similaires pour les parents dont l'enfant réside en dehors de l'espace économique européen est discriminatoire. En effet, cette mesure introduit une inégalité de traitement entre les parents selon le lieu de résidence de leur enfant, car il n'est pas justifié que la contribution financière à l'éducation et au bien-être d'un enfant soit reconnue fiscalement lorsque celui-ci vit dans l'Espace économique européen, mais pas lorsqu'il réside ailleurs dans le monde. Par ailleurs, cette mesure touche particulièrement les familles issues de l'immigration, qui sont statistiquement plus susceptibles d'avoir des enfants vivant en dehors de l'EEE. Or, le principe d'égalité devant l'impôt suppose que des contribuables placés dans une situation comparable (ici, des parents séparés qui versent une pension alimentaire) soient traités de manière équitable, indépendamment du pays de résidence de leur enfant. En conséquence, le présent amendement a pour objet de supprimer ces dispositions discriminatoires.

M. Lode Vereeck et M. Wouter Vermeersch (VB) présentent l'amendement n° 104/partim (DOC 56 0963/028) tendant à supprimer l'article 32 du présent projet de loi.

Cette mesure est jugée antisociale, injuste et inefficace. La réduction de la déductibilité des pensions alimentaires de 80 % à 70 %, puis à 60 % et enfin à 50 % entraîne une baisse du revenu disponible pour le débiteur et sa nouvelle famille éventuelle. Un nombre important de décisions judiciaires actuellement en vigueur concernant les pensions alimentaires devront être révisées à court terme afin d'adapter le montant des pensions alimentaires actuellement versées ou accordées à la lumière des dispositions concernées en discussion. Cela entraînera la judiciarisation des accords familiaux et de nouveaux conflits entre les parents, dont les enfants feront les frais. De plus, la surcharge de travail de la justice risque d'entraîner une grande insécurité juridique. Aujourd'hui, les délais d'attente devant les tribunaux de la famille sont déjà de 6 à 9 ans.

Dit amendement tot weglating van artikel 32 strekt ertoe de rechtszekerheid van de onderhoudsgeldregeling te vrijwaren.

De heer François De Smet (DéFI) dient *amendement nr. 61/partim* (DOC 56 0963/021) in, tot weglating van artikel 33 van dit wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 32.

De heer Lode Vereeck en de heer Wouter Vermeersch (VB) dienen *amendement nr. 104/partim* (DOC 56 0963/028) in, tot weglating van artikel 33 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 32.

De heer François De Smet (DéFI) dient *amendement nr. 61/partim* (DOC 56 0963/021) in, tot weglating van artikel 34 van dit wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 32.

De heer Lode Vereeck en de heer Wouter Vermeersch (VB) dienen *amendement nr. 104/partim* (DOC 56 0963/028) in, tot weglating van artikel 34 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 32.

De heer François De Smet (DéFI) dient *amendement nr. 61/partim* (DOC 56 0963/021) in, tot weglating van artikel 35 van dit wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 32.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen *amendement nr. 95* (DOC 56 0963/028) in, tot vervanging van artikel 35 van het wetsontwerp.

Zoals aangegeven in het advies van de Inspectie van Financiën kan de familierechtbank bij de berekening van het bedrag van de onderhoudsuitkeringen ingevolge een echtscheiding rekening houden met de aftrekbaarheid en de belastbaarheid ten belope van 80 %. Het valt niet uit te sluiten dat dit ook het geval is voor de afspraken inzake onderhoudsuitkeringen in het raam van een echtscheiding met onderlinge toestemming. Onvermijdelijk zal een aanzienlijk aantal van de in kracht van gewijsde gegane rechterlijke uitspraken over onderhoudsuitkeringen op

L'amendement visant à supprimer cet article tend à sauvegarder la sécurité juridique du système des pensions alimentaires.

M. François De Smet (DéFI) présente l'*amendement n° 61/partim* (DOC 56 0963/021) tendant à supprimer l'article 33 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 32.

M. Lode Vereeck et M. Wouter Vermeersch (VB) présentent l'*amendement n° 104/partim* (DOC 56 0963/028) tendant à supprimer l'article 33 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 32.

M. François De Smet (DéFI) présente l'*amendement n° 61/partim* (DOC 56 0963/021) tendant à supprimer l'article 34 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 32.

M. Lode Vereeck et M. Wouter Vermeersch (VB) présentent l'*amendement n° 104/partim* (DOC 56 0963/028) tendant à supprimer l'article 34 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 32.

M. François De Smet (DéFI) présente l'*amendement n° 61/partim* (DOC 56 0963/021) tendant à supprimer l'article 35 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 32.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'*amendement n° 95* (DOC 56 0963/028) tendant à remplacer l'article 35 du présent projet de loi.

Comme indiqué dans l'avis de l'Inspection des finances, le calcul du montant des pensions alimentaires versées à la suite d'un divorce par le tribunal de la famille peut tenir compte de la déductibilité et de l'imposition à hauteur de 80 % de celles-ci. Il n'est pas exclu que cela soit également le cas pour les accords relatifs aux pensions alimentaires conclus dans le cadre d'un divorce par consentement mutuel. Il est donc inévitable qu'un nombre considérable de décisions judiciaires actuellement en vigueur en matière de pensions alimentaires

korte termijn moeten worden herzien om het bedrag van de onderhoudsuitkeringen dat momenteel wordt betaald of toegekend, aan te passen aan de ontworpen regeling. Zowel de betrokken partijen als de familierechtbanken worden bijgevolg geconfronteerd met een situatie waarin snel moet worden opgetreden om in te spelen op de gevolgen van de ontworpen regeling, waarop zij zich niet konden voorbereiden.

In haar verslag wijst de Inspectie van Financiën er overigens op dat ook de inschakeling van de Dienst voor Alimentatievorderingen daar gevolgen van kan ondervinden, omdat plots wijzigende fiscale omstandigheden de betaling van de onderhoudsuitkeringen zouden kunnen bemoeilijken.

Dit amendement wijzigt de toepassing in de tijd van de voorgestelde maatregel. Die moet immers voorzienbaar zijn voor iedere betrokkene bij een regeling omtrent onderhoudsuitkeringen, opdat tijdig de nodige voorbereidingen kunnen worden getroffen.

De heer Lode Vereeck en de heer Wouter Vermeersch (VB) dienen amendement nr. 104/partim (DOC56 0963/028) in, tot weglating van artikel 35 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 32.

Afdeling 7

Bestaansmiddelen van personen ten laste

Art. 36 tot 39

Over deze artikelen worden geen opmerkingen gemaakt.

Afdeling 8

Indexering van fiscale uitgaven

Art. 40

Over dit artikel worden geen opmerkingen gemaakt.

Art. 41

Mevrouw Charlotte Verkeyn c.s. dient amendement nr. 63 (DOC 56 0963/022) in, dat ertoe strekt in het ontworpen artikel 41 een punt c/1) in te voegen.

devront être révisées à très court terme afin d'adapter le montant des pensions alimentaires actuellement versées ou accordées à la lumière du projet de règlement. Tant les parties concernées que les tribunaux de la famille sont donc confrontés à une situation qui exige une action rapide en raison des conséquences du projet de règlement auquel ils n'ont pas pu se préparer.

Le rapport de l'Inspection des finances souligne d'ailleurs à cet égard les conséquences possibles pour le recours au Service des créances alimentaires, car le paiement des pensions alimentaires pourrait être moins bien respecté en raison de l'évolution soudaine de la situation fiscale.

Cet amendement modifie l'application dans le temps de la mesure proposée. En effet, l'application dans le temps de la mesure proposée doit être prévisible pour toute personne concernée par un accord relatif à une pension alimentaire, afin que les préparatifs nécessaires puissent être effectués en temps utile.

M. Lode Vereeck et M. Wouter Vermeersch (VB) présentent l'amendement n° 104/partim (DOC 56 0963/028) tendant à supprimer l'article 35 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 32.

Section 7

Ressource de personnes à charge

Art. 36 à 39

Les articles 36 à 39 ne font l'objet d'aucune discussion.

Section 8

Indexation des dépenses fiscales

Art. 40

L'article 40 ne fait l'objet d'aucune discussion.

Art. 41

Mme Charlotte Verkeyn et consorts présentent l'amendement n° 63 (DOC 56 0963/022) tendant à ajouter dans l'article 41 un c/1) dans le présent projet de loi.

Dit amendement brengt een technische correctie aan in artikel 178, § 3, WIB 92. De verwijzing naar het derde lid van artikel 178, § 3, WIB 92 in het bestaande vierde lid van die paragraaf (dat het vijfde lid wordt) moet worden aangepast, omdat een nieuw lid wordt ingevoegd tussen het tweede en derde lid. Deze wijziging is, net als de andere wijzigingen die door artikel 41 worden aangebracht, van toepassing vanaf het aanslagjaar 2026. De bepaling met betrekking tot de inwerkingtreding hoeft dus niet te worden aangepast.

De heer François De Smet (DéFI) dient vervolgens amendement nr. 62 (DOC 56 0963/021) in, dat ertoe strekt het bepaalde onder e) weg te laten uit artikel 41 van het wetsontwerp.

De weg te laten bepaling onder e) had als doel het bepaalde onder 3°/1 van paragraaf 5 van artikel 178 van het Wetboek van de inkomstenbelastingen 1992 (WIB 92) te vervangen. Dit amendement strekt ertoe die wijziging niet door te voeren en dus het bepaalde onder 3°/1 onveranderd te laten. Teneinde werkloosheidsvallen tegen te gaan, stelt de regering voor om het maximumbedrag van het belastingkrediet voor kinderen ten laste te bevriezen tot het bedrag dat voor het aanslagjaar 2025 geldt, namelijk 550 euro per kind ten laste. Dat bedrag staat in artikel 134, § 3, tweede lid, eerste streepje, WIB 92. De niet-indexering ervan wordt geregeld in artikel 178, § 5, 3°/1, WIB 92. De betrokken ouders ontvangen momenteel een belastingkrediet. Dat betekent dat de FOD Financiën hun dat bedrag stort, bijvoorbeeld wanneer een alleenstaande ouder niet werkt of een zeer laag inkomen heeft dat deels uit onderhoudsgeld bestaat. Het bedrag van dat belastingkrediet wordt beperkt tot 550 euro per kind ten laste (inkomstenjaar 2024, aanslagjaar 2025). Die mogelijkheid om de verhoging van de belastingvrije som in een terugstortbaar belastingkrediet om te zetten, is voor de financieel kwetsbaarste gezinnen een noodzakelijke fiscale steun waarmee ze hun gezinsbudget kunnen aanvullen, zelfs al wordt dat belastingkrediet geplafonneerd. Voorts wordt een bijkomende verhoging van de belastingvrije som toegekend voor elk kind jonger dan 3 jaar wanneer de ouders geen kinderopvangkosten aangeven (omdat hun kind niet naar de kinderopvang gaat). Het betreft momenteel een bedrag van 720 euro (aanslagjaar 2025, inkomstenjaar 2024). Ouders met een laag inkomen die zelf voor de opvang van hun kinderen zorgen, zullen bijgevolg ook niet langer ten volle voordeel uit die financiële steunmaatregel halen, aangezien het belastingkrediet niet meer wordt geïndexeerd. Dat betekent dat het reële inkomen van de kwetsbaarste gezinnen zal dalen.

Volgens de Ligue des Familles is het een volstrekte illusie te denken dat die ouders door de afschaffing van dat belastingvoordeel makkelijker opnieuw de weg naar

Cet amendement apporte une modification technique à l'article 178, § 3, CIR 92. La référence à l'alinéa 3 de l'article 178, § 3, CIR 92 dans l'actuel alinéa 4 (qui devient l'alinéa 5) de ce paragraphe, doit être adaptée en raison de l'insertion d'un nouvel alinéa entre le deuxième et le troisième alinéa de ce paragraphe. Tout comme les autres modifications apportées par l'article 41, cette modification est également applicable à partir de l'exercice d'imposition 2026. La disposition relative à l'entrée en vigueur ne doit dès lors pas être adaptée.

M. François De Smet (DéFI) présente ensuite l'amendement n° 62 (DOC 56 0963/021) tendant à supprimer dans l'article 41 du présent projet de loi le e).

Le e) supprimé avait pour objet de remplacer le 3°/1 du paragraphe 5 de l'article 178 du Code des impôts sur les revenus 1992 (CIR 92). Le présent amendement supprime cette modification et laisse donc ce 3°/1 inchangé. Afin d'éviter des pièges à l'emploi, le gouvernement propose de geler le montant maximum du crédit d'impôt pour enfants à charge au montant applicable pour l'exercice d'imposition 2025, c.-à.-d. 550 euros par enfant à charge. Ce montant est inscrit dans l'article 134, § 3, alinéa 2, premier tiret du CIR 92. Sa non-indexation est réglée dans l'article 178, § 5, 3°/1, du CIR 92. Les parents concernés reçoivent actuellement un crédit d'impôt, c'est-à-dire que le SPF Finances leur verse cette somme, par exemple si un parent seul ne travaille pas ou perçoit des revenus très faibles dont une partie provient de la pension alimentaire. Le montant de ce crédit d'impôt est limité à 550 euros par enfant à charge (revenus 2024, exercice d'imposition 2025). Cette possibilité de convertir la majoration de la quotité exemptée en crédit d'impôt remboursable permet aux familles plus précarisées de bénéficier de ce soutien fiscal nécessaire pour le budget de leur ménage, même si celui-ci est plafonné. Une majoration supplémentaire de la quotité exemptée d'impôt est par ailleurs accordée pour chaque enfant de moins de 3 ans quand les parents ne déclarent pas de frais de garde d'enfant (quand leur enfant ne va pas en crèche). Ce montant est actuellement de 720 euros (exercice d'imposition 2025, revenus 2024). Les parents qui ont peu de revenus et gardent eux-mêmes leur enfant ne bénéficieront dès lors plus non plus pleinement de cette mesure de soutien financier, puisque le crédit d'impôt ne sera plus indexé. Ceci signifie que le revenu réel des familles les plus précaires sera réduit.

Pour la Ligue des Familles, il est totalement illusoire de penser que la suppression de cet avantage fiscal incitera ces parents à rejoindre plus facilement le marché

de arbeidsmarkt zullen vinden. Aangezien er nu reeds een tekort aan plaatsen in de kinderopvang heerst en alleenstaande ouders of ouders die niet op hulp van familie kunnen rekenen, zo al moeilijker aan een baan geraken, zal dat hen zeker niet lukken met een verlaging van hun gezinsinkomen. Dit amendement beoogt de door besparingen ingegeven boude verlaging van de steun aan kwetsbare gezinnen weg te laten, aangezien dat verlies niet op een andere manier wordt gecompenseerd.

Art. 42

Over dit artikel worden geen opmerkingen gemaakt.

Afdeling 9

DBI-aftrek en DBI-beveks

Onderafdeling 1

Groepsbijdrage

Art. 43

Over dit artikel worden geen opmerkingen gemaakt.

Onderafdeling 2

DBI-beveks

Art. 44 tot 48

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 96/partim (DOC 56 0963/028) in, dat ertoe strekt artikel 44 weg te laten.

De DBI-bevekstaks is na de meerwaardebelasting de zoveelste taks op vrije beroepers en ondernemers. Arizona zou beter taksen afschaffen dan er in te voeren.

Ondernemers zijn geen CEO's die zichzelf een minimumloon uitkeren vanuit hun ligstoel aan het zwembad van hun villa.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 96/partim (DOC 56 0963/028) in, dat ertoe strekt artikel 45 weg te laten.

du travail. Dans un contexte de pénurie de places en crèche et d'accès à l'emploi de plus en plus difficile pour les parents solo ou sans soutien familial, réduire le revenu des ménages ne leur permettra pas davantage qu'aujourd'hui d'accéder à l'emploi. Le présent amendement vise donc à supprimer ce qui constitue une réduction pure et simple des aides destinées aux familles vulnérables, en vue d'économies budgétaires, sans que soit compensée cette perte.

Art. 42

L'article 42 ne fait l'objet d'aucune discussion.

Section 9

Déduction RDT et SICAV RDT

Sous-section 1^{re}

Transfert intra-groupe

Art. 43

L'article 43 ne fait l'objet d'aucune discussion.

Sous-section 2

SICAV-RDT

Art. 44 à 48

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 96/partim (DOC 56 0963/028) tendant à supprimer l'article 44 du présent projet de loi.

Après la taxe sur les plus-values, la taxe sur les SICAV/RDT est une nouvelle taxe imposée aux professions libérales et aux entrepreneurs. L'Arizona ferait mieux de supprimer les taxes plutôt que d'en introduire de nouvelles.

Les entrepreneurs ne sont pas des CEO qui se versent un salaire minimum, tout en se reposant au bord de la piscine de leur villa.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 96/partim (DOC 56 0963/028) tendant à supprimer l'article 45 du présent projet de loi.

Er wordt verwezen naar de verantwoording van het amendement op artikel 44.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 96/partim (DOC 56 0963/028) in, dat ertoe strekt artikel 46 weg te laten.

Er wordt verwezen naar de verantwoording van het amendement op artikel 44.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 96/partim (DOC 56 0963/028) in, dat ertoe strekt artikel 47 weg te laten.

Er wordt verwezen naar de verantwoording van het amendement op artikel 44.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 96/partim (DOC 56 0963/028) in, dat ertoe strekt artikel 48 weg te laten.

Er wordt verwezen naar de verantwoording van het amendement op artikel 44.

Afdeling 10

*Wijzigingen betreffende het belastingkrediet
voor eigen middelen*

Art. 49

Over dit artikel worden geen opmerkingen gemaakt.

Art. 50

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 50 van het wetsontwerp.

De lijst van Arizonataksen bevat uitsluitend pestmaatregelen voor mensen die werken, sparen en ondernemen. Een hele reeks verlagingen van de belastinggrondslag wordt afgeschaft, waardoor de koopkracht de facto daalt. Volgens de indieners is alleen de opheffing van de belastingvermindering voor huisbedienden een relevante maatregel. De andere belastingen gaan beter omlaag dan omhoog.

Il est renvoyé à la justification développée à l'article 44.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 96/partim (DOC 56 0963/028) tendant à supprimer l'article 46 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 44.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 96/partim (DOC 56 0963/028) tendant à supprimer l'article 47 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 44.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 96/partim (DOC 56 0963/028) tendant à supprimer l'article 48 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 44.

Section 10

*Modifications relatives au crédit d'impôt
pour moyens propres*

Art. 49

L'article 49 ne fait l'objet d'aucune discussion.

Art. 50

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 50 du présent projet de loi.

La liste des taxes de la coalition *Arizona* est un ensemble de mesures punitives pour les personnes qui travaillent, épargnent et entreprennent. Il s'agit de toute une série de réductions de la base imposable qui sont supprimées et de facto engendrent une diminution du pouvoir d'achat. À part celle relative au personnel de maison, que l'auteur juge pertinente, il estime qu'il vaut mieux réduire les impôts au lieu de les augmenter.

Afdeling 11*Vereenvoudiging van de belastingaangifte***Onderafdeling 1***Wijzigingen van het Wetboek
van de inkomstenbelastingen 1992***Art. 51 tot 65**

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 51 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 52 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 53 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 54 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 55 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 56 van het wetsontwerp.

Section 11*Simplification de la déclaration fiscale***Sous-section 1^{re}***Modifications du Code
des impôts sur les revenus 1992***Art. 51 à 65**

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 51 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 52 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 53 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 54 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 55 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 56 du présent projet de loi.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 57 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 58 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 59 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 60 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 61 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Lode Vereeck en de heer Wouter Vermeersch (VB) dienen amendement nr. 105/partim (DOC 56 0963/028) in, tot weglating van artikel 61 van het wetsontwerp.

Het is economisch onzinnig en fiscaal onrechtvaardig om belastingen te heffen op minwaarden. De belastingvermindering moet dus behouden blijven.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 62 van het wetsontwerp.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 57 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 58 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 59 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 60 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 61 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Lode Vereeck et M. Wouter Vermeersch (VB) présentent l'amendement n° 105 (DOC 56 0963/028) tendant à supprimer l'article 61 du présent projet de loi.

Il est économiquement absurde et fiscalement injuste d'imposer les moins-values. La réduction d'impôt doit donc être maintenue.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 62 du présent projet de loi.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 63 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 64 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 65 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

Art. 66

Over dit artikel worden geen opmerkingen gemaakt.

Art. 67 tot 84

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 67 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 68 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 69 van het wetsontwerp.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 63 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 64 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 65 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

Art. 66

L'article 66 ne fait l'objet d'aucune discussion.

Art. 67 à 84

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 67 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 68 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 69 du présent projet de loi.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 70 van het wetsontwerp.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 71 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 72 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 73 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 74 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 75 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

Mevrouw Charlotte Verkeyn c.s. dient amendement nr. 64 (DOC 56 0963/022) in, dat ertoe strekt in artikel 76 het punt a) te vervangen en in het punt c) woorden te vervangen.

Dit amendement brengt een aantal technische correcties aan in artikel 76 van het wetsontwerp om onder

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 70 du présent projet de loi.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 71 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 72 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 73 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 74 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 75 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

Mme Charlotte Verkeyn et consorts présentent l'amendement n° 64 (DOC 56 0963/022) tendant à remplacer dans l'article 76 le a) et à remplacer des mots dans le c).

Cet amendement apporte quelques modifications techniques à l'article 76 du projet de loi afin de tenir

meer rekening te houden met de opheffing van artikel 145⁵⁰, WIB 92.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 76 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 77 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 78 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 79 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 80 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 81 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

Mevrouw Charlotte Verkeyn c.s. dient amendement nr. 65 (DOC 56 0963/022) in, dat ertoe strekt in titel 2, hoofdstuk 1, afdeling 11, onderafdeling 1, een artikel 81/1 in te voegen.

compte, entre autres, de l'abrogation de l'article 145⁵⁰, CIR 92.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 76 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 77 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 78 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 79 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 80 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 81 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

Mme Charlotte Verkeyn et consorts présentent l'amendement n° 65 (DOC 56 0963/022) tendant à ajouter dans le titre 2, chapitre 1^{er}, section 11, sous-section 1^{re} un article 81/1 (nouveau).

Artikel 531, WIB 92 bepaalt dat artikel 67, § 4, WIB 92, dat de terugname regelt van de vrijstelling voor bijkomend personeel voor wetenschappelijk onderzoek en de uitbouw van het technologisch potentieel van de onderneming, verder van toepassing blijft. Artikel 67 WIB 92 wordt door deze wet opgeheven vanaf het aanslagjaar 2027. De verwijzing naar artikel 67, § 4, WIB 92 in artikel 531 WIB 92 moet dan ook expliciet betrekking hebben op artikel 67, § 4, WIB 92 zoals het bestond vooraleer het door deze wet werd opgeheven.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 82 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 83 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 84 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

Onderafdeling 2

Wijzigingen van de wet van 1 juni 2008 houdende de invoering van een belastingvermindering voor aandelen in ontwikkelingsfondsen voor microfinanciering in ontwikkelingslanden en houdende de vaststelling van de voorwaarden voor de erkenning als ontwikkelingsfonds

Art. 85 en 86

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 85 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

L'article 531 du CIR 92 stipule que l'article 67, § 4, CIR 92, qui régit la reprise de l'exonération pour personnel supplémentaire affecté à la recherche scientifique et au développement du potentiel technologique de l'entreprise, reste d'application. L'article 67 du CIR 92 est abrogé par la présente loi à partir de l'exercice d'imposition 2027. Dès lors, la référence à l'article 67, § 4, CIR 92 dans l'article 531 CIR 92 doit être fixée à l'article 67, § 4, CIR 92 tel qu'il existait avant son abrogation par la présente loi.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 82 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 83 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 84 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

Sous-section 2

Modifications de la loi du 1^{er} juin 2008 instaurant une réduction d'impôt pour les participations sous la forme d'actions dans des fonds de développement du micro-financement dans les pays en développement et fixant les conditions d'agrément en tant que fonds de développement

Art. 85 et 86

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 85 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 97/partim (DOC 56 0963/028) in, tot weglating van artikel 86 van het wetsontwerp.

Er wordt verwezen naar de verantwoording van het amendement op artikel 50.

Onderafdeling 3

Inwerkingtreding

Art. 87

Mevrouw Charlotte Verkeyn c.s. dient amendement nr. 66 (DOC 56 0963/022) in, dat ertoe strekt in artikel 87, vijfde lid, van het wetsontwerp woorden te vervangen.

De wijziging van artikel 531 WIB 92 moet, net als de opheffing van artikel 67 WIB 92, in werking treden vanaf het aanslagjaar 2027.

Mevrouw Charlotte Verkeyn c.s. dient amendement nr. 67 (DOC 56 0963/022) in, dat ertoe strekt in artikel 87, vierde lid, van het wetsontwerp woorden te vervangen.

Artikel 70 van het ontwerp wijzigt artikel 171 WIB 92 om rekening te houden met de opheffing van een aantal belastingverminderingen vanaf het aanslagjaar 2026. Dit amendement voegt in artikel 87, vierde lid, van het ontwerp een verwijzing in naar artikel 70 van het ontwerp, vermits de wijzigingen van artikel 171 WIB 92 eveneens in werking moeten treden vanaf het aanslagjaar 2026.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 98 (DOC 56 0963/028) in, tot vervanging van artikel 87, eerste lid, van het wetsontwerp.

In belastingzaken is er geen plaats voor retroactiviteit. Het amendement beoogt de inwerkingtreding van de regeling te corrigeren uit hoofde van het beginsel van de voorspelbaarheid.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 99 (DOC 56 0963/028) in, tot vervanging van artikel 87, tweede lid, van het wetsontwerp.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 97/partim (DOC 56 0963/028) tendant à supprimer l'article 86 du présent projet de loi.

Il est renvoyé à la justification développée à l'article 50.

Sous-section 3

Entrée en vigueur

Art. 87

Mme Charlotte Verkeyn et consorts présentent l'amendement n° 66 (DOC 56 0963/022) tendant à remplacer des mots dans l'article 87, alinéa 5 du présent projet de loi.

La modification de l'article 531, CIR 92 doit, tout comme l'abrogation de l'article 67 du CIR 92, entrer en vigueur à partir de l'exercice d'imposition 2027.

Mme Charlotte Verkeyn et consorts présentent ensuite l'amendement n° 67 (DOC 56 0963/022) tendant à remplacer des mots dans l'article 87, alinéa 4 du présent projet de loi.

L'article 70 du projet modifie l'article 171, CIR 92 afin de tenir compte de l'abrogation d'un nombre de réductions d'impôt à partir de l'exercice d'imposition 2026. Le présent amendement insère dans l'article 87, alinéa 4, du projet une référence à l'article 70 du projet, étant donné que les modifications de l'article 171, CIR 92 doivent également entrer en vigueur à partir de l'exercice d'imposition 2026.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 98 (DOC 56 0963/028) tendant à remplacer l'alinéa 1^{er} dans l'article 87 du présent projet de loi.

Il n'y a pas de place pour la rétroactivité en matière fiscale. L'amendement vise à corriger l'entrée en vigueur du dispositif en vertu du principe de prévisibilité.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 99 (DOC 56 0963/028) tendant à remplacer l'alinéa 2 dans l'article 87 du présent projet de loi.

In belastingzaken is er geen plaats voor retroactiviteit. Het amendement beoogt de inwerkingtreding van de regeling te corrigeren uit hoofde van het beginsel van de voorspelbaarheid.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 100 (DOC 56 0963/028) in, tot vervanging van artikel 87, derde lid, van het wetsontwerp.

In belastingzaken is er geen plaats voor retroactiviteit. Het amendement beoogt de inwerkingtreding van de regeling te corrigeren uit hoofde van het beginsel van de voorspelbaarheid.

HOOFDSTUK 2

Procedure

Afdeling 1

Wijzigingen aangebracht aan de aanslag- en onderzoekstermijnen van het Wetboek van de inkomstenbelastingen 1992

Art. 87/1 (*nieuw*) tot 90

Over de artikelen 87/1 (*nieuw*) tot 90 worden geen opmerkingen gemaakt.

Afdeling 2

Wijzigingen aangebracht aan de verjaringstermijnen voor de vordering tot voldoening van de belasting in het Wetboek van de belasting over de toegevoegde waarde

Art. 90/1 (*nieuw*) tot 92

Over de artikelen 90/1 (*nieuw*) tot 92 worden geen opmerkingen gemaakt.

Art. 93

Mevrouw Charlotte Verkeyn c.s. dient amendement nr. 68 (DOC 56 0963/022) in, dat ertoe strekt de inleidende zin in artikel 93 van dit wetsontwerp te vervangen.

De bedoeling daarvan is te verduidelijken dat de vervanging van artikel 84*ter* van het Btw-Wetboek, zoals bepaald in artikel 93, moet plaatsvinden na de

Il n'y a pas de place pour la rétroactivité en matière fiscale. L'amendement vise à corriger l'entrée en vigueur du dispositif en vertu du principe de prévisibilité.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 100 (DOC 56 0963/028) tendant à remplacer l'alinéa 3 dans l'article 87 du présent projet de loi.

Il n'y a pas de place pour la rétroactivité en matière fiscale. L'amendement vise à corriger l'entrée en vigueur du dispositif en vertu du principe de prévisibilité.

CHAPITRE 2

Procédure

Section 1^{re}

Modifications apportées aux délais d'imposition et d'investigation du Code des impôts sur les revenus 1992

Art. 87/1 (*nouveau*) à 90

Les articles 87/1 (*nouveau*) à 90 ne font l'objet d'aucune discussion.

Section 2

Modifications apportées aux délais de prescription de l'action en recouvrement de la taxe dans le Code de la taxe sur la valeur ajoutée

Art. 90/1 (*nouveau*) à 92

Les articles 90/1 (*nouveau*) à 92 ne font l'objet d'aucune discussion.

Art. 93

Mme Charlotte Verkeyn et consorts présentent l'amendement n° 68 (DOC 56 0963/022) tendant à remplacer la phrase liminaire dans l'article 93 du présent projet de loi.

Cet amendement modifie la phrase liminaire de l'article 93 du projet afin de préciser que le remplacement de l'article 84*ter*, du Code TVA tel que prévu dans ledit

vervanging van artikel 84^{ter} van het Btw-Wetboek door artikel 56 van de wet van 12 mei 2024.

Art. 94 en 95

Over de artikelen 94 en 95 worden geen opmerkingen gemaakt.

HOOFDSTUK 3 (NIEUW)

Wijziging van het Wetboek diverse rechten en taksen, teneinde bepaalde ambtenaren toegang te geven tot het Centraal Aanspreekpunt van de Nationale Bank van België

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 77 (DOC 56 0963/028) in, tot weglating van hoofdstuk 3 van het wetsontwerp.

Overwegende advies nr. 36/2025 van de Gegevensbeschermingsautoriteit, waarin wordt beklemtoond dat de integratie van het Centraal Aanspreekpunt (CAP) in het datawarehouse van de FOD Financiën voor doeleinden van datamining een ernstige inmenging in het fundamentele recht op privacy vormt en waarin wordt aanbevolen specifieke waarborgen in te voeren inzake proportionaliteit, finaliteit en transparantie;

Overwegende advies nr. 77.807/2-3 van de Raad van State van 1 juli 2025, waarin de Raad stelt dat de essentiële elementen van de verwerking van persoonsgegevens, zoals de finaliteit, de categorieën van verwerkte gegevens, de personen die er toegang toe hebben en de bewaartermijn, duidelijk in de wettelijke norm zelf moeten worden vastgelegd;

Overwegende Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144, en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (verordening artificiële intelligentie), de zogenoemde AI Act, die de lidstaten verplicht erop toe te zien dat het gebruik van hoogrisico-AI-systemen door overheidsinstanties voldoet aan de beginselen van transparantie, traceerbaarheid en daadwerkelijke menselijke controle;

article 93, doit intervenir après le remplacement de l'article 84^{ter}, Code TVA, par l'article 56 de la loi du 12 mai 2024.

Art. 94 et 95

Les articles 94 et 95 ne font l'objet d'aucune discussion.

CHAPITRE 3 (NOUVEAU)

Modification du Code des droits et taxes divers visant à octroyer à certains fonctionnaires l'accès au point de contact central de la Banque Nationale de Belgique

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 77 (DOC 56 0963/028) tendant à supprimer le chapitre 3 du présent projet de loi.

Considérant l'avis n° 36/2025 de l'Autorité de protection des données, qui souligne que l'intégration du Point de contact central (PCC) dans l'entrepôt de données du SPF Finances à des fins d'exploration de données constitue une ingérence grave dans le droit fondamental à la vie privée et recommande la mise en place de garanties spécifiques en matière de proportionnalité, de finalité et de transparence;

Considérant l'avis n° 77.807/2-3 du Conseil d'État du 1^{er} juillet 2025, qui insiste sur le fait que les éléments essentiels du traitement des données à caractère personnel, tels que la finalité, les catégories de données traitées, les personnes ayant accès à ces données et la durée de conservation, doivent être clairement définis dans la norme légale elle-même;

Considérant le règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle), dit "AI Act", adopté par le Parlement européen et le Conseil, qui oblige les États membres à veiller à ce que l'utilisation de systèmes d'IA à haut risque par les autorités publiques respecte les principes de transparence, de traçabilité et de contrôle humain effectif;

Gelet op de recente werkzaamheden van de Raad van Europa, met name in het raam van het Kaderverdrag inzake artificiële intelligentie, mensenrechten, democratie en de rechtsstaat (2024), waarin wordt benadrukt dat het gebruik van algoritmische systemen door overheden begrijpelijk, verklaarbaar en aan onafhankelijk toezicht onderworpen moet zijn, teneinde het democratisch vertrouwen en het respect voor de rechtsstaat te waarborgen;

strekt dit amendement tot opheffing van de tekst omdat de datamining bij het CAP niet voldoet aan de basisprincipes zoals die gelden in het fiscaal wetboek (cfr. het “perverse” doel van de datamining waar in het advies van de GBA naar wordt verwezen) en voorts ook omdat die datamining reactief is. Het CAP kan overeenkomstig het fiscaal wetboek (artikel 322 WIB § 3, WIB 1992) enkel worden ingekeken onder dezelfde voorwaarden als die welke gelden voor de opheffing van het bankgeheim, met name:

1. indien een fiscaal onderzoek ten aanzien van een bepaalde belastingplichtige aanwijzingen oplevert dat de betrokkene fraude pleegt; en

2. indien de belastingplichtige in kwestie weigert mee te werken door niet binnen een maand te reageren op een vraag om inlichtingen.

Aangezien datamining inhoudt dat CAP-gegevens worden geraadpleegd zonder enig fiscaal onderzoek ten aanzien van een belastingplichtige, zonder enige aanwijzing van fraude en zonder dat er sprake is van een weigering tot medewerking, moet de opname van het CAP in het datawarehouse worden verhinderd.

Art. 95/1 (*nieuw*) en 95/2 (*nieuw*)

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 78 (DOC 56 0963/028) in, tot weglating van artikel 95/1 (nieuw) van het wetsontwerp.

Er wordt verwezen naar de verantwoording van amendement nr. 77.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 89 (DOC 56 0963/028) in, tot vervanging van artikel 95/1 (nieuw) van het wetsontwerp.

Er wordt verwezen naar de verantwoording van amendement nr. 77.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen amendement nr. 90

Considérant les travaux récents du Conseil de l'Europe, notamment dans le cadre de la convention-cadre sur l'intelligence artificielle, les droits de l'homme, la démocratie et l'État de droit (2024), qui soulignent que l'utilisation de systèmes algorithmiques par les pouvoirs publics doit être compréhensible, explicable et soumise à un contrôle indépendant, afin de garantir la confiance démocratique et le respect de l'État de droit;

Cet amendement supprime le texte, car le data mining au CAP ne respecte pas les principes fondamentaux applicables dans le code fiscal (cf. l'objectif “perverse” du data mining évoqué par l'APD dans son avis) et parce qu'il est réactif. Le CAP ne peut être consulté dans le code fiscal (article 322 CIR § 3 CIR 1992) que dans les mêmes conditions que celles prévues pour la levée du secret bancaire, à savoir:

1. si une enquête fiscale concernant un contribuable donné révèle l'existence d'indices de fraude de la part de ce contribuable; et

2. si celui-ci refuse de coopérer en répondant à une demande de renseignements dans un délai d'un mois.

Étant donné que le data mining implique la consultation de ces données CAP sans qu'il y ait d'enquête fiscale à l'égard d'un contribuable, sans qu'il y ait d'indice de fraude et sans qu'il y ait de refus de coopérer, l'intégration du CAP dans l'entrepôt de données doit être empêchée.

Art. 95/1 (*nouveau*) et 95/2 (*nouveau*)

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 78 (DOC 56 0963/028) tendant à supprimer l'article 95/1 (nouveau) du présent projet de loi.

Il est renvoyé à la justification développée à l'amendement n° 77.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 89 (DOC 56 0963/028) tendant à remplacer le texte de l'article 95/1 (nouveau) du présent projet de loi.

Il est renvoyé à la justification développée à l'amendement n° 77.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'amendement n° 90

(DOC 56 0963/028) in, teneinde artikel 95/1 (*nieuw*) van het wetsontwerp aan te vullen met een paragraaf 3.

Er wordt verwezen naar de verantwoording van amendement nr. 77.

De heer Vincent Van Quickenborne en mevrouw Alexia Bertrand (Open Vld) dienen *amendement nr. 79* (DOC 56 0963/028) in, tot weglating van artikel 95/2 (*nieuw*) van het wetsontwerp.

Er wordt verwezen naar de verantwoording van amendement nr. 77.

HOOFDSTUK 4 (*NIEUW*)

Wijziging van de wet van 3 augustus 2012 houdende bepalingen betreffende de verwerking van persoonsgegevens door de Federale Overheidsdienst Financiën in het kader van zijn opdrachten

De heer Van Quickenborne en mevrouw Bertrand dienen *amendement nr. 80* (DOC 56 0963/028) in, tot weglating van hoofdstuk 4 (*nieuw*). Voor de verantwoording wordt verwezen naar amendement nr. 77 en naar de algemene bespreking.

Art. 95/3 (*nieuw*)

De heer Van Quickenborne en mevrouw Bertrand dienen *amendement nr. 81* (DOC 56 0963/028) in, tot weglating van artikel 95/3 (*nieuw*). Voor de verantwoording wordt verwezen naar amendement nr. 77 en naar de algemene bespreking.

De heer Van Quickenborne en mevrouw Bertrand dienen *amendement nr. 88* (DOC 56 0963/028) in, teneinde artikel 95/3 (*nieuw*) te vervangen en aan te vullen met een paragraaf 4.

Dit amendement stelt een betere formulering voor, teneinde nietigverklaring door het Grondwettelijk Hof te voorkomen. Paragraaf 1 verduidelijkt het doel van datamining door te specificeren dat alleen de gegevens die het CAP vanaf 1 januari 2026 qontvangt in de datawarehouse zullen worden ingebracht, wat elke vorm van terugwerkende kracht uitsluit.

Daarnaast beoogt het amendement een paragraaf 4 in te voegen, teneinde te verzekeren dat de informatie van het CAP op evenredige, controleerbare en wettige wijze wordt gebruikt, door een wettelijk verankerde grendel in te stellen met betrekking tot het depseudonimiseren

(DOC 56 0963/028) tendant à compléter l'article 95/1 (*nouveau*) du présent projet de loi par un paragraphe 3.

Il est renvoyé à la justification développée à l'amendement n° 77.

M. Vincent Van Quickenborne et Mme Alexia Bertrand (Open Vld) présentent l'*amendement n° 79* (DOC 56 0963/028) tendant à supprimer l'article 95/2 (*nouveau*) du présent projet de loi.

Il est renvoyé à la justification développée à l'amendement n° 77.

CHAPITRE 4 (*NOUVEAU*)

Modification de la loi du 3 août 2012 portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions

M. Van Quickenborne et Mme Bertrand présentent l'*amendement n° 80* (DOC 56 0963/028) tendant à supprimer le chapitre 4 (*nouveau*). Pour la justification, il est renvoyé à l'amendement n° 77 et à la discussion générale.

Art. 95/3 (*nouveau*)

M. Van Quickenborne et Mme Bertrand présentent l'*amendement n° 81* (DOC 56 0963/028) tendant à supprimer l'article 95/3 (*nouveau*). Pour la justification, il est renvoyé à l'amendement n° 77 et à la discussion générale.

M. Van Quickenborne et Mme Bertrand présentent l'*amendement n° 88* (DOC 56 0963/028) tendant à remplacer l'article 95/3 (*nouveau*) et à le compléter par un § 4.

Le présent amendement propose une rédaction renforcée afin de prévenir toute annulation par la Cour constitutionnelle. Le § 1^{er} clarifie l'objet du *data mining* en précisant que seules les données reçues du PCC à partir du 1^{er} janvier 2026 seront versées dans le datawarehouse, ce qui exclut toute rétroactivité.

En outre, l'amendement tend à insérer un § 4 visant à assurer une utilisation proportionnée, contrôlable et légale des informations du PCC, en introduisant un verrou légal sur la depseudonymisation des données, laquelle doit rester strictement limitée aux situations de fraude

van gegevens. Depseudonimisatie moet immers strikt beperkt blijven tot situaties van ernstige fiscale fraude. Die toevoeging beoogt ook te voorzien in een voorafgaande menselijke interventie, overeenkomstig de vereisten inzake transparantie en menselijk toezicht, zoals opgelegd door de GBA, de Raad van State en de Europese en internationale normen. Die maatregel komt tegemoet aan de noodzaak om het democratische vertrouwen in het werk van de belastingdiensten te behouden.

De volgende paragrafen van het gewijzigde artikel beogen te bepalen dat de bevoegde controledienst zijn onafhankelijkheid behoudt om te beslissen of hij al dan niet een controle uitvoert, en ze verduidelijken de aard van de informatie die via datamining wordt verkregen. Tot slot bevestigt de gewijzigde tekst dat noch de selectie via datamining, noch de mededeling ervan aan de controlediensten enig rechtsgevolg heeft voor de belastingplichtige.

De heer Van Quickenborne en mevrouw Bertrand dienen *amendement nr. 101* (DOC 56 0963/028) in, dat ertoe strekt in artikel 95/3 een paragraaf 3/1 in te voegen.

Dit amendement strekt ertoe het gebruik van artificiële intelligentie door de belastingdiensten bij de verwerking van gegevens, met name gegevens afkomstig van het CAP, strikt te reguleren. Het beoogt tevens tegemoet te komen aan de bezorgdheden van de GBA en aan de Europese normen op het stuk van de onverklaarbaarheid en het gebrek aan democratische controle over AI-systemen die worden toegepast op gevoelige financiële gegevens, en beoogt te waarborgen dat de FOD Financiën alleen deterministische, gedocumenteerde en verifieerbare verwerkingen kan uitvoeren die strikt gebaseerd zijn op goedgekeurde criteria. Voorts strekt het ertoe de invoering van disproportionele algoritmische toezichtmechanismen te voorkomen en zo het vertrouwen van de burgers en de legitimiteit van de fraudebestrijding te versterken.

Dit amendement sluit aan bij de logica van de Europese verordening inzake artificiële intelligentie (Verordening (EU) 2024/1689) en heeft tot doel elke onduidelijkheid inzake de toepasselijkheid ervan op administratieve handelingen of handelingen van strafrechtelijke aard te voorkomen. De rechtspraak van het Hof van Cassatie heeft immers al bevestigd dat bepaalde fiscale beschikkingen een strafrechtelijk karakter kunnen hebben, wat een hoger niveau van waarborgen vereist. Tot slot beoogt het amendement de governance aan te scherpen, door voor elke technische ontwikkeling een impactanalyse en een onafhankelijke controle verplicht te stellen.

fiscale grave. Cet ajout vise également la mise en place d'une intervention humaine préalable, conformément aux exigences de transparence et de contrôle humain édictées par l'APD, le Conseil d'État ainsi que par les normes européennes et internationales. Cette mesure répond à la nécessité de préserver la confiance démocratique dans l'action de l'administration fiscale. Il vise enfin à répondre à la nécessité de préserver la confiance démocratique dans l'action de l'administration fiscale.

Les paragraphes suivants du texte modifié précisent que le service de contrôle compétent conserve son indépendance pour décider d'engager ou non un contrôle, et clarifient la nature des informations issues du *data mining*. Enfin, le texte modifié confirme que ni la sélection par *data mining*, ni sa communication aux services de contrôle n'ont d'effet juridique pour le contribuable.

M. Van Quickenborne et Mme Bertrand présentent l'*amendement n° 101* (DOC 56 0963/028) tendant à insérer un § 3/1 dans l'article 95/3 (*nouveau*).

Le présent amendement vise à encadrer strictement l'utilisation de l'intelligence artificielle par l'administration fiscale dans le cadre du traitement des données, notamment celles issues du PCC. Il tend également à répondre aux préoccupations de l'APD et aux normes européennes concernant l'inexplicabilité et le manque de contrôle démocratique des systèmes d'IA appliqués à des données financières sensibles, et vise à garantir que le SPF Finances ne pourra effectuer que des traitements déterministes, documentés et vérifiables, strictement fondés sur des critères approuvés. Il tend en outre à empêcher l'introduction de mécanismes de surveillance algorithmique disproportionnés, renforçant ainsi la confiance des citoyens et la légitimité de la lutte contre la fraude.

Cet amendement s'inscrit dans la logique de l'AI Act (EU 2024/1689) et vise à prévenir toute ambiguïté quant à son applicabilité aux actes administratifs ou aux actes à caractère pénal. En effet, la jurisprudence de la Cour de cassation a déjà reconnu que certaines décisions fiscales peuvent revêtir un caractère pénal, ce qui impose un niveau de garantie renforcé. Enfin, il vise à consolider la gouvernance en imposant la réalisation d'une analyse d'impact et un contrôle indépendant pour toute évolution technique.

De heren Vereeck en Vermeersch dienen amendement nr. 106 (DOC 56 0963/028) in, dat ertoe strekt artikel 95/3 weg te laten.

Dit amendement beoogt de handhaving van de bestaande procedure, die alle nodige waarborgen biedt op het gebied van grondrechten en eerbiediging van de rechtsstaat. De huidige procedure bepaalt dat toegang tot de gegevens van het CAP alleen kan worden verleend nadat er een concreet vermoeden van fraude bestaat en de belastingplichtige in gebreke is gesteld, waarbij laatstgenoemde een maand de tijd krijgt om toelichting te verstrekken. Dat mechanisme waarborgt de bescherming van het beginsel van het vermoeden van onschuld, alsook het recht op privacy en de procedurele transparantie. Het gaat de risico's die verbonden zijn aan ondoorzichtige of geautomatiseerde systemen uit de weg, terwijl de belastingdienst toch gebruik kan maken van verklaarbare en evenredige dataminingtechnieken. In tegenstelling tot de in het wetsontwerp voorgestelde regeling waarborgt de huidige procedure dat de belastingplichtige wordt ingelicht over de redenen waarom hij werd geselecteerd en de mogelijkheid op weerwoord behoudt vooraleer er ingrijpende maatregelen worden genomen. Derhalve strekt dit amendement ertoe de nieuwe bepalingen weg te laten en de bestaande regeling, die doeltreffend werkt en in overeenstemming is met de grondwettelijke beginselen, te handhaven.

HOOFDSTUK 5 (NIEUW)

Wijzigingen van de wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van rekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest

De heer Van Quickenborne en mevrouw Bertrand dienen amendement nr. 82 (DOC 56 0963/028) in, tot weglating van hoofdstuk 5 (nieuw). Voor de verantwoording wordt verwezen naar amendement nr. 77 en naar de algemene bespreking.

Art. 95/4 (nieuw)

De heer Van Quickenborne en mevrouw Bertrand dienen amendement nr. 83 (DOC 56 0963/028) in, tot weglating van artikel 95/4 (nieuw). Voor de verantwoording wordt verwezen naar amendement nr. 77 en naar de algemene bespreking.

MM. Vereeck et Vermeersch présentent l'amendement n° 106 (DOC 56 0963/028) tendant à supprimer l'article 95/3 (nouveau).

Le présent amendement propose de maintenir la procédure existante, qui offre toutes les garanties nécessaires en matière de droits fondamentaux et de respect de l'État de droit. La procédure actuelle prévoit qu'un accès aux données du PCC ne peut être accordé qu'après l'existence d'un soupçon concret de fraude et la mise en demeure du contribuable, lequel dispose d'un délai d'un mois pour fournir des explications. Ce mécanisme assure la protection du principe de présomption d'innocence, ainsi que des droits à la vie privée et à la transparence procédurale. Il évite les risques liés à des systèmes opaques ou automatisés, tout en permettant à l'administration de recourir à des techniques de *data mining* explicables et proportionnées. Contrairement au dispositif proposé dans le projet de loi à l'examen, la procédure actuelle garantit que le contribuable est informé des raisons de sa sélection et conserve la possibilité de répondre avant toute mesure intrusive. En conséquence, le présent amendement tend à supprimer les nouvelles dispositions et à confirmer le maintien du cadre existant, qui fonctionne efficacement et respecte les principes constitutionnels.

CHAPITRE 5 (NOUVEAU)

Modifications de la loi du 8 juillet 2018 portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt

M. Van Quickenborne et Mme Bertrand présentent l'amendement n° 82 (DOC 56 0963/028) tendant à supprimer le chapitre 5 (nouveau). Pour la justification, il est renvoyé à l'amendement n° 77 et à la discussion générale.

Art. 95/4 (nouveau)

M. Van Quickenborne et Mme Bertrand présentent l'amendement n° 83 (DOC 56 0963/028) tendant à supprimer l'article 95/4 (nouveau). Pour la justification, il est renvoyé à l'amendement n° 77 et à la discussion générale.

Art. 95/5 (*nieuw*)

De heer Van Quickenborne en mevrouw Bertrand dienen amendement nr. 84 (DOC 56 0963/028) in, tot weglating van artikel 95/5 (*nieuw*). Voor de verantwoording wordt verwezen naar amendement nr. 77 en naar de algemene bespreking.

Art. 95/6 (*nieuw*)

De heer Van Quickenborne en mevrouw Bertrand dienen amendement nr. 85 (DOC 56 0963/028) in, tot weglating van artikel 95/6 (*nieuw*). Voor de verantwoording wordt verwezen naar amendement nr. 77 en naar de algemene bespreking.

Art. 95/7 (*nieuw*)

De heer Van Quickenborne en mevrouw Bertrand dienen amendement nr. 86 (DOC 56 0963/028) in, tot weglating van artikel 95/7 (*nieuw*). Voor de verantwoording wordt verwezen naar amendement nr. 77 en naar de algemene bespreking.

Art. 95/8 (*nieuw*)

De heer Van Quickenborne en mevrouw Bertrand dienen amendement nr. 87 (DOC 56 0963/028) in, tot weglating van artikel 95/8 (*nieuw*). Voor de verantwoording wordt verwezen naar amendement nr. 77 en naar de algemene bespreking.

Art. 95/9 (*nieuw*)

De heren Vereeck en Vermeersch dienen amendement nr. 107 (DOC 56 0963/028) in, tot invoeging van een artikel 95/9 (*nieuw*).

Dit amendement beoogt de transparantie en traceerbaarheid te waarborgen van geautomatiseerde beslissingen inzake dossierselectie. Het bepaalt dat selectie door middel van datamining geenszins een voldoende grondslag kan vormen voor een bestuurlijke beslissing of een fiscale sanctie. Die regel bestaat reeds, maar moet worden aangevuld met een transparantieverplichting met betrekking tot de selectiefase zelf.

Het amendement stelt daarom voor dat aan de geselecteerde belastingplichtige een tegenfeitelijke verklaring moet worden verstrekt. In die verklaring moeten de factoren staan die tot de selectie hebben geleid en moet worden aangegeven hoe de situatie had verschild

Art. 95/5 (*nouveau*)

M. Van Quickenborne et Mme Bertrand présentent l'amendement n° 84 (DOC 56 0963/028) tendant à supprimer l'article 95/5 (*nouveau*). Pour la justification, il est renvoyé à l'amendement n° 77 et à la discussion générale.

Art. 95/6 (*nouveau*)

M. Van Quickenborne et Mme Bertrand présentent l'amendement n° 85 (DOC 56 0963/028) tendant à supprimer l'article 95/6 (*nouveau*). Pour la justification, il est renvoyé à l'amendement n° 77 et à la discussion générale.

Art. 95/7 (*nouveau*)

M. Van Quickenborne et Mme Bertrand présentent l'amendement n° 86 (DOC 56 0963/028) tendant à supprimer l'article 95/7 (*nouveau*). Pour la justification, il est renvoyé à l'amendement n° 77 et à la discussion générale.

Art. 95/8 (*nouveau*)

M. Van Quickenborne et Mme Bertrand présentent l'amendement n° 87 (DOC 56 0963/028) tendant à supprimer l'article 95/8 (*nouveau*). Pour la justification, il est renvoyé à l'amendement n° 77 et à la discussion générale.

Art. 95/9 (*nouveau*)

MM. Vereeck et Vermeersch présentent l'amendement n° 107 (DOC 56 0963/028) tendant à insérer un article 95/9 (*nouveau*).

Le présent amendement vise à garantir la transparence et la traçabilité des décisions automatisées de sélection des dossiers. Il précise que la sélection par *data mining* ne peut, en aucun cas, constituer une base suffisante pour une décision administrative ou pour une sanction fiscale. Cette règle est déjà prévue, mais elle doit être complétée par une obligation de transparence concernant la phase de sélection elle-même.

L'amendement propose donc d'imposer la communication d'une explication contrefactuelle au contribuable sélectionné. Cette explication doit contenir les éléments qui ont conduit à sa sélection et mentionner comment la situation aurait été différente si certains facteurs avaient

indien bepaalde factoren anders waren geweest. Op die manier wordt inzicht verschaft dat ook begrijpelijk is zonder diepgaande technische kennis en wordt beter uitgelegd waarom de werkwijze terecht is.

Art. 95/10 (*nieuw*)

De heren Vereeck en Vermeersch dienen amendement nr. 108 (DOC 56 0963/028) in, tot invoeging van een artikel 95/10.

Dit amendement beoogt te regelen hoe gegevens van belastingplichtigen mogen worden gebruikt voor de ontwikkeling en training van door de belastingdiensten toegepaste modellen voor datamining en artificiële intelligentie. Het bepaalt dat de belastingdiensten gegevens uit dossiers van belastingplichtigen niet mogen gebruiken voor het kalibreren, optimaliseren of trainen van algoritmen zonder de uitdrukkelijke en voorafgaande toestemming van de betrokken belastingplichtige. Die in het amendement voorgestelde bepaling is gebaseerd op de Europese beginselen inzake gegevensbescherming en transparantie, zoals vastgelegd in de AVG en herhaald in de AI Act (EU 2024/1689). Aldus wordt tegemoetgekomen aan de noodzaak het fundamentele recht van de belastingplichtige te waarborgen dat hij controle behoudt over het gebruik van zijn persoonsgegevens, in het bijzonder wanneer die worden ingezet voor secundaire doeleinden zoals de verbetering van geautomatiseerde selectiesystemen. De maatregel vormt een minimale garantie voor democratie en eerbiediging van de privacy, terwijl belastingplichtigen die dat wensen toch vrijwillig kunnen bijdragen aan de verbetering van de instrumenten voor een krachtigere fraudedetectie.

HOOFDSTUK 6 (*NIEUW*)

Maaltijdcheques

Mevrouw Verkeyn c.s. dient amendement nr. 72 (DOC 56 0963/027) in, tot invoeging van een hoofdstuk 6 in titel II van het wetsontwerp.

Het amendement strekt ertoe werkgevers en werknemers rechtszekerheid te geven door het Wetboek van de inkomstenbelastingen 1992 aan te passen aan de geplande verhoging van het maaltijdchequebedrag. Dankzij die aanpassing blijft de koopkracht van de werknemers gevrijwaard en is de samenhang tussen de sociale regelgeving en het toepasbare fiscaal stelsel gewaarborgd.

De heer Van Quickenborne dient amendement nr. 69 (DOC 56 0963/026) in, tot invoeging van

été modifiés. Ce mécanisme permet une compréhension accessible sans connaissance technique approfondie et renforce la légitimité du processus.

Art. 95/10 (*nouveau*)

*MM. Vereeck et Vermeersch présentent l'amendement n° 108 (DOC 56 0963/028) tendant à insérer un article 95/10 (*nouveau*).*

Le présent amendement vise à encadrer l'utilisation des données des contribuables dans le cadre du développement et de l'entraînement des modèles de *data mining* ou d'intelligence artificielle utilisés par l'administration fiscale. Il prévoit que la fiscalité ne peut utiliser les données issues des dossiers des contribuables à des fins de calibration, d'optimisation ou d'entraînement des algorithmes sans le consentement explicite et préalable de l'intéressé. Cette disposition proposée par l'amendement s'inspire des principes européens en matière de protection des données et de transparence, tels que consacrés par le RGPD et rappelés dans l'AI Act (UE 2024/1689). Elle répond à la nécessité de garantir le droit fondamental du contribuable à contrôler l'usage de ses données personnelles, en particulier lorsqu'elles sont utilisées pour des finalités secondaires, comme l'amélioration des systèmes automatisés de sélection. Cette mesure constitue un minimum de garantie démocratique et de respect de la vie privée, tout en laissant la possibilité aux contribuables favorables à une détection renforcée de la fraude de contribuer volontairement à l'amélioration des outils.

CHAPITRE 6 (*NOUVEAU*)

Titres-repas

*Mme Verkeyn et consorts présentent l'amendement n° 72 (DOC 56 0963/027) tendant à insérer un chapitre 6 (*nouveau*) dans le titre II du projet de loi.*

Le présent amendement vise à garantir la sécurité juridique des employeurs et des travailleurs en adaptant le Code des impôts sur les revenus 1992 à l'augmentation prévue de la valeur des titres-repas. Cette adaptation permettra de préserver le pouvoir d'achat des travailleurs et d'assurer la cohérence entre la réglementation sociale et le régime fiscal applicable.

M. Van Quickenborne présente l'amendement n° 69 (DOC 56 0963/026) tendant à insérer un chapitre 6

een hoofdstuk 6 betreffende de maaltijdcheques in titel II van het wetsontwerp. Voor de verantwoording wordt verwezen naar artikel 95/9 (*nieuw*) en naar de algemene bespreking.

Art. 95/9 (*nieuw*)

Mevrouw Verkeyn c.s. dient amendement nr. 73 (DOC 56 0963/027) in, tot invoeging van een artikel 95/9.

Het amendement strekt ertoe artikel 38/1, § 2, eerste lid, 5°, van het WIB 92 aan te passen, teneinde het maximumbedrag van de werkgeversbijdrage in elektronische maaltijdcheques te verhogen van 6,91 naar 8,91 euro.

De heer Van Quickenborne dient amendement nr. 69 (DOC 56 0963/026) in, tot invoeging van een artikel 95/9.

Het amendement strekt ertoe dringende maatregelen te nemen om de koopkracht van de burgers te ondersteunen. Vanaf 1 januari 2026 wordt het maximumbedrag van de werkgeversbijdrage in de maaltijdcheques verhoogd van 6,91 euro naar 8,91 euro, wat de totale waarde van een maaltijdcheque op 10 euro brengt. Die maatregel veronderstelt de wijziging van artikel 38/1, § 2, eerste lid, 5°, van het Wetboek van de inkomstenbelastingen 1992 (WIB 92). Dankzij die verhoging houdt een voltijdse werknemer jaarlijks ongeveer 400 euro netto extra over. Bovendien wordt het bedrag van het als beroepskosten aftrekbare deel van de werkgever verdubbeld van 2 naar 4 euro per maaltijdcheque wanneer de werkgeversbijdrage het nieuwe maximumbedrag bereikt (wijziging van artikel 53, 14°, WIB 92). Is de werkgeversbijdrage lager dan dat maximum, dan blijft de het fiscaal aftrekbare bedrag maximaal 2 euro per maaltijdcheque.

Art. 95/10 (*nieuw*)

Mevrouw Verkeyn c.s. dient amendement nr. 74 (DOC 56 0963/027) in, tot invoeging van een artikel 95/10.

Het amendement beoogt rechtszekerheid te bieden aan de werkgevers in geval van een verhoging van het maximumbedrag van de werkgeversbijdrage voor maaltijdcheques. Overeenkomstig het regeerakkoord wordt de fiscale aftrekbaarheid van maaltijdcheques voor de werkgevers dienovereenkomstig aangepast: het bedrag dat aftrekbaar is als beroepskosten wordt verdubbeld van 2 naar 4 euro per maaltijdcheque wanneer de werkgeversbijdrage het nieuwe plafond van 8,91 euro

(*nouveau*) relatif aux titres-repas dans le titre II du projet de loi. Pour la justification, il est renvoyé à l'article 95/9 (*nouveau*) et à la discussion générale.

Art. 95/9 (*nouveau*)

*Mme Verkeyn et consorts présentent l'amendement n° 73 (DOC 56 0963/027) tendant à insérer un article 95/9 (*nouveau*).*

Le présent amendement vise à adapter l'article 38/1, § 2, alinéa 1^{er}, 5°, CIR 92 afin d'augmenter le montant maximum de l'intervention de l'employeur dans les titres-repas électroniques de 6,91 à 8,91 euros.

*M. Van Quickenborne présente l'amendement n° 69 (DOC 56 0963/026) tendant à insérer un article 95/9 (*nouveau*).*

Le présent amendement vise à prendre des mesures urgentes pour soutenir le pouvoir d'achat des citoyens. À partir du 1^{er} janvier 2026, le montant maximal de la contribution de l'employeur dans les titres-repas est porté de 6,91 euros à 8,91 euros, ce qui porte la valeur totale du titre-repas à 10 euros. Cette mesure implique la modification de l'article 38/1, § 2, alinéa 1^{er}, 5°, du Code des impôts sur les revenus 1992 (CIR 92). Pour un travailleur à temps plein, cette augmentation représente un gain annuel d'environ 400 euros nets. En outre, le montant de l'intervention déductible à titre de frais professionnels est doublé et passe de 2 euros à 4 euros par titre-repas lorsque la contribution patronale atteint le nouveau maximum (modification de l'article 53, 14°, CIR 92). Si la contribution patronale est inférieure à ce maximum, la déduction reste plafonnée à 2 euros par titre-repas.

Art. 95/10 (*nouveau*)

*Mme Verkeyn et consorts présentent l'amendement n° 74 (DOC 56 0963/027) tendant à insérer un article 95/10 (*nouveau*).*

Le présent amendement vise à assurer la sécurité juridique des employeurs en cas d'augmentation du montant maximum de l'intervention de l'employeur dans les titres-repas. Conformément à l'accord de gouvernement, la déductibilité fiscale des titres-repas dans le chef de l'employeur est adaptée en conséquence: le montant déductible à titre de frais professionnels est doublé et passe de 2 euros à 4 euros par titre-repas lorsque la contribution patronale atteint le nouveau plafond de

bereikt. Als de werkgever een tussenkomst toekent die lager is dan dat plafond, blijft de aftrek beperkt tot 2 euro per maaltijdcheque. Die maatregel garandeert fiscale coherentie en rechtszekerheid voor de werkgevers, en ondersteunt tegelijk de verhoging van de waarde van maaltijdcheques tot 10 euro.

De heer Van Quickenborne dient amendement nr. 70 (DOC 56 0963/026) in, dat ertoe strekt een artikel 95/10 in te voegen. Voor de verantwoording wordt verwezen naar amendement nr. 69 en naar de algemene bespreking.

Art. 95/11 (nieuw)

Mevrouw Verkeyn c.s. dient amendement nr. 75 (DOC 56 0963/027) in, tot invoeging van een artikel 95/11.

Het amendement beoogt de nieuwe bedragen van toepassing te maken op de elektronische maaltijdcheques die worden toegekend vanaf 1 januari 2026.

De heer Van Quickenborne dient amendement nr. 71 (DOC 56 0963/026) in, dat ertoe strekt een artikel 95/11 in te voegen. Voor de verantwoording wordt verwezen naar amendement nr. 69 en naar de algemene bespreking.

Art. 95/12 (nieuw)

De heer Van Quickenborne en mevrouw Bertrand dienen amendement nr. 76 (DOC 56 0963/028) in, dat ertoe strekt een artikel 95/12 in te voegen.

Dit amendement beoogt de transparantie en de bevattelijkheid van de wettelijke bepalingen te verbeteren door de term “CAP” stelselmatig te vervangen door de woorden “money control” in de wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van rekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest, alsook in het voorliggende wetsontwerp. Deze terminologische wijziging geeft een getrouwer beeld van het doel van de regeling, namelijk het controleren van financiële stromen, en zorgt ervoor dat de burgers en de betrokken actoren dat aspect beter begrijpen.

8,91 euros. Si l'employeur octroie une intervention inférieure à ce plafond, la déduction reste limitée à 2 euros par titre-repas. Cette mesure garantit la cohérence fiscale et la sécurité juridique pour les employeurs tout en accompagnant l'augmentation de la valeur des titres-repas à 10 euros.

M. Van Quickenborne présente l'amendement n° 70 (DOC 56 0963/026) tendant à insérer un article 95/10 (nouveau). Pour la justification, il est renvoyé à l'amendement n° 69 et à la discussion générale.

Art. 95/11 (nouveau)

Mme Verkeyn et consorts présentent l'amendement n° 75 (DOC 56 0963/027) tendant à insérer un article 95/11 (nouveau).

Le présent amendement vise à rendre applicables les nouveaux montants aux titres-repas électroniques qui sont attribués à partir du 1^{er} janvier 2026.

M. Van Quickenborne présente l'amendement n° 71 (DOC 56 0963/026) tendant à insérer un article 95/11 (nouveau). Pour la justification, il est renvoyé à l'amendement n° 69 et à la discussion générale.

Art. 95/12 (nouveau)

M. Van Quickenborne et Mme Bertrand présentent l'amendement n° 76 (DOC 56 0963/028) tendant à insérer un article 95/12 (nouveau).

Le présent amendement vise à renforcer la transparence et la lisibilité des dispositions légales en remplaçant systématiquement la dénomination “PCC” par “money control” dans la loi du 30 juillet 2018 portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt, ainsi que dans le projet de loi à l'examen. Cette modification terminologique permet de refléter plus fidèlement la finalité du dispositif, à savoir le contrôle des flux financiers, et d'assurer une meilleure compréhension par les citoyens et les acteurs concernés.

IV. — STEMMINGEN

TITEL 1

Algemene bepaling

Artikel 1

Artikel 1 wordt eenparig aangenomen.

TITEL 2

Financiën

HOOFDSTUK 1

Wijzigingen betreffende de inkomstenbelastingen**Afdeling 1***Vastgoedfiscaliteit*

Art. 2 tot 10

Artikel 2 wordt aangenomen met 9 tegen 3 stemmen en 2 onthoudingen.

De artikelen 3 tot 10 worden achtereenvolgens aangenomen met 9 tegen 2 stemmen en 3 onthoudingen.

Art. 11

Amendement nr. 102 (*partim*) wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

Artikel 11 wordt aangenomen met 9 tegen 3 stemmen en 2 onthoudingen.

Art. 12

Artikel 12 wordt aangenomen met 9 tegen 2 stemmen en 3 onthoudingen.

Art. 13

Amendement nr. 102 (*partim*) wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

Artikel 13 wordt aangenomen met 9 tegen 3 stemmen en 2 onthoudingen.

IV. — VOTES

*Titre 1^{er}**Disposition générale*Article 1^{er}

L'article 1^{er} est adopté à l'unanimité.

TITRE 2

*Finances*CHAPITRE 1^{ER}**Modifications relatives aux impôts sur les revenus****Section 1^{re}***Fiscalité immobilière*

Art. 2 à 10

L'article 2 est adopté par 9 voix contre 3 et 2 abstentions.

Les articles 3 à 10 sont successivement adoptés par 9 voix contre 2 et 3 abstentions.

Art. 11

L'amendement n° 102 (*partim*) est rejeté par 12 voix contre une et une abstention.

L'article 11 est adopté par 9 voix contre 3 et 2 abstentions.

Art. 12

L'article 12 est adopté par 9 voix contre 2 et 3 abstentions.

Art. 13

L'amendement n° 102 (*partim*) est rejeté par 12 voix contre une et une abstention.

L'article 13 est adopté par 9 voix contre 3 et 2 abstentions.

Art. 14

Amendement nr. 91 wordt verworpen met 11 stemmen tegen 1 en 2 onthoudingen.

Artikel 14 wordt aangenomen met 9 tegen 2 stemmen en 3 onthoudingen.

Afdeling 2

*Ingekomen belastingplichtigen en
ingekomen onderzoekers*

Art. 15

Amendement nr. 103 (*partim*) wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

Artikel 15 wordt aangenomen met 10 tegen 4 stemmen.

Art. 16

Amendement nr. 103 (*partim*) wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

Artikel 16 wordt aangenomen met 10 tegen 4 stemmen.

Art. 16/1 (*nieuw*)

Artikel 16/1 (*nieuw*) wordt aangenomen met 10 tegen 4 stemmen.

Art. 17

Artikel 17 wordt aangenomen met 10 tegen 4 stemmen.

Afdeling 3

Flexi-jobs

Art. 18 en 19

De artikelen 18 en 19 worden achtereenvolgens aangenomen met 11 tegen 3 stemmen.

Art. 19/1 tot 19/9 (*nieuw*)

Amendement nr. 92, dat ertoe strekt de artikelen 19/1 tot 19/9 (*nieuw*) in te voegen, wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

Art. 14

L'amendement n° 91 est rejeté par 11 voix contre une et 2 abstentions.

L'article 14 est adopté par 9 voix contre 2 et 3 abstentions.

Section 2

*Contribuables impatriés et
chercheurs impatriés*

Art. 15

L'amendement n° 103 (*partim*) est rejeté par 12 voix contre une et une abstention.

L'article 15 est adopté par 10 voix contre 4.

Art. 16

L'amendement n° 103 (*partim*) est rejeté par 12 voix contre une et une abstention.

L'article 16 est adopté par 10 voix contre 4.

Art. 16/1 (*nouveau*)

L'article 16/1 (*nouveau*) est adopté par 10 voix contre 4.

Art. 17

L'article 17 est adopté par 10 voix contre 4.

Section 3

Flexi-jobs

Art. 18 et 19

Les articles 18 et 19 sont successivement adoptés par 11 voix contre 3.

Art. 19/1 à 19/9 (*nouveaux*)

L'amendement n° 92 tendant à insérer les articles 19/1 à 19/9 est rejeté par 12 voix contre une et une abstention.

Art. 20

Amendement nr. 93 wordt ingetrokken.

Artikel 20 wordt aangenomen met 11 tegen 3 stemmen.

Afdeling 4*Autofiscaliteit*

Art. 21 tot 26

De artikelen 21 tot 23 worden achtereenvolgens aangenomen met 9 tegen 2 stemmen en 3 onthoudingen.

Artikel 24 wordt aangenomen met 9 tegen 3 stemmen en 2 onthoudingen.

De artikelen 25 en 26 worden achtereenvolgens aangenomen met 9 tegen 2 stemmen en 3 onthoudingen.

Art. 26/1 (*nieuw*)

Artikel 26/1 (*nieuw*) wordt aangenomen met 9 tegen 2 stemmen en 3 onthoudingen.

Art. 27

Artikel 27 wordt aangenomen met 9 tegen 2 stemmen en 3 onthoudingen.

Art. 27/1 (*nieuw*)

Amendement nr. 94, dat een artikel 27/1 (*nieuw*) invoegt, wordt verworpen met 12 tegen 2 stemmen.

Afdeling 5*Investeringsaftrek*

Art. 28 tot 31

De artikelen 28 tot 31 worden achtereenvolgens 11 tegen 2 stemmen en 1 onthouding.

Art. 20

L'amendement n° 93 est retiré.

L'article 20 est adopté par 11 voix contre 3.

Section 4*Fiscalité automobile*

Art. 21 à 26

Les articles 21 à 23 sont successivement adoptés par 9 voix contre 2 et 3 abstentions.

L'article 24 est adopté par 9 voix contre 3 et 2 abstentions.

Les articles 25 et 26 sont successivement adoptés par 9 voix contre 2 et 3 abstentions.

Art. 26/1 (*nouveau*)

L'article 26/1 (*nouveau*) est adopté par 9 voix contre 2 et 3 abstentions.

Art. 27

L'article 27 est adopté par 9 voix contre 2 et 3 abstentions.

Art. 27/1 (*nouveau*)

L'amendement n° 94 tendant à insérer un article 27/1 est rejeté par 12 voix contre 2.

Section 5*Déduction pour investissement*

Art. 28 à 31

Les articles 28 à 31 sont successivement adoptés par 11 voix contre 2 et une abstention.

Afdeling 6*Onderhoudsuitkeringen***Art. 32**

Amendement nr. 61 (*partim*) wordt verworpen met 9 tegen 4 stemmen en 1 onthouding.

Amendement nr. 104 (*partim*) wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

Artikel 32 wordt aangenomen met 9 tegen 5 stemmen.

Art. 33

Amendement nr. 61 (*partim*) wordt verworpen met 9 tegen 4 stemmen en 1 onthouding.

Amendement nr. 104 (*partim*) wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

Artikel 33 wordt aangenomen met 9 tegen 5 stemmen.

Art. 34

Amendement nr. 61 (*partim*) wordt verworpen met 9 tegen 4 stemmen en 1 onthouding.

Amendement nr. 104 (*partim*) wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

Artikel 34 wordt aangenomen met 9 tegen 5 stemmen.

Art. 35

Amendement nr. 61 (*partim*) wordt verworpen met 9 tegen 4 stemmen en 1 onthouding.

Amendement nr. 104 (*partim*) wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

Amendement nr. 95 wordt verworpen met 10 tegen 3 stemmen en 1 onthouding.

Artikel 35 wordt aangenomen met 9 tegen 5 stemmen.

Section 6*Rentes alimentaires***Art. 32**

L'amendement n° 61 (*partim*) est rejeté par 9 voix contre 4 et une abstention.

L'amendement n° 104 (*partim*) est rejeté par 12 voix contre une et une abstention.

L'article 32 est adopté par 9 voix contre 5.

Art. 33

L'amendement n° 61 (*partim*) est rejeté par 9 voix contre 4 et une abstention.

L'amendement n° 104 (*partim*) est rejeté par 12 voix contre une et une abstention.

L'article 33 est adopté par 9 voix contre 5.

Art. 34

L'amendement n° 61 (*partim*) est rejeté par 9 voix contre 4 et une abstention.

L'amendement n° 104 (*partim*) est rejeté par 12 voix contre une et une abstention.

L'article 34 est adopté par 9 voix contre 5.

Art. 35

L'amendement n° 61 (*partim*) est rejeté par 9 voix contre 4 et une abstention.

L'amendement n° 104 (*partim*) est rejeté par 12 voix contre une et une abstention.

L'amendement n° 95 est rejeté par 10 voix contre 3 voix et une abstention.

L'article 35 est adopté par 9 voix contre 5.

Afdeling 7*Bestaansmiddelen van personen ten laste*

Art. 36 tot 39

De artikelen 36 tot 39 worden achtereenvolgens aangenomen met 11 tegen 3 stemmen.

Afdeling 8*Indexering van fiscale uitgaven*

Art. 40

Artikel 40 wordt aangenomen met 9 tegen 4 stemmen en 1 onthouding.

Art. 41

Amendement nr. 62 wordt verworpen met 9 tegen 3 stemmen en 2 onthoudingen.

Amendement nr. 63 wordt aangenomen met 9 stemmen en 5 onthoudingen.

Artikel 41, aldus geamendeerd, wordt aangenomen met 9 tegen 3 stemmen en 2 onthoudingen.

Art. 42

Artikel 42 wordt aangenomen met 9 tegen 3 stemmen en 2 onthoudingen.

Afdeling 9*DBI-aftrek en DBI-beveks**Onderafdeling 1**Groepsbijdrage*

Art. 43

Artikel 43 wordt aangenomen met 12 tegen 2 stemmen.

Section 7*Ressources de personnes à charge*

Art. 36 à 39

Les articles 36 à 39 sont successivement adoptés par 11 voix contre 3.

Section 8*Indexation de dépenses fiscales*

Art. 40

L'article 40 est adopté par 9 voix contre 4 et une abstention.

Art. 41

L'amendement n° 62 est rejeté par 9 voix contre 3 et 2 abstentions.

L'amendement n° 63 est adopté par 9 voix et 5 abstentions.

L'article 41, ainsi modifié, est adopté par 9 voix contre 3 et 2 abstentions.

Art. 42

L'article 42 est adopté par 9 voix contre 3 et 2 abstentions.

Section 9*Déduction RDT et SICAV RDT**Sous-section 1^{re}**Transfert intra-groupe*

Art. 43

L'article 43 est adopté par 12 voix contre 2.

*Onderafdeling 2**DBI-beveks*

Art. 44 tot 48

Amendement nr. 96 *partim* wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

De artikelen 44 tot 48 worden achtereenvolgens aangenomen met 11 stemmen tegen 1 en 2 onthoudingen.

Afdeling 10*Wijzigingen betreffende het belastingkrediet voor eigen middelen*

Art. 49 en 50

De artikelen 49 en 50 worden achtereenvolgens aangenomen met 11 stemmen tegen 1 en 2 onthoudingen.

Afdeling 11*Vereenvoudiging van de belastingaangifte**Onderafdeling 1**Wijzigingen van het Wetboek van de inkomstenbelastingen 1992*

Art. 51 en 52

Amendement nr. 97 *(partim)* wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

De artikelen 51 en 52 worden achtereenvolgens aangenomen met 10 tegen 2 stemmen en 2 onthoudingen.

Art. 53

Amendement nr. 97 *(partim)* wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

Artikel 53 wordt aangenomen met 10 tegen 4 stemmen.

Art. 54 tot 60

Amendement nr. 97 *(partim)* wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

*Sous-section 2**SICAV-RDT*

Art. 44 à 48

L'amendement n° 96 *(partim)* est rejeté par 12 voix contre une et une abstention.

Les articles 44 à 48 sont successivement adoptés par 11 voix contre une et 2 abstentions.

Section 10*Modifications relatives au crédit d'impôt pour moyens propres*

Art. 49 et 50

Les articles 49 et 50 sont successivement adoptés par 11 voix contre une et 2 abstentions.

Section 11*Simplification de la déclaration fiscale**Sous-section 1^{re}**Modifications du Code des impôts sur les revenus 1992*

Art. 51 et 52

L'amendement n° 97 *(partim)* est rejeté par 12 voix contre une et une abstention.

Les articles 51 et 52 sont successivement adoptés par 10 voix contre 2 et 2 abstentions.

Art. 53

L'amendement n° 97 *(partim)* est rejeté par 12 voix contre une et une abstention.

L'article 53 est adopté par 10 voix contre 4.

Art. 54 à 60

L'amendement n° 97 *(partim)* est rejeté par 12 voix contre une et une abstention.

De artikelen 54 tot 60 worden achtereenvolgens aangenomen met 10 tegen 2 stemmen en 2 onthoudingen.

Art. 61

Amendement nr. 97 (*partim*) wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

Amendement nr. 105 wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

Artikel 61 wordt aangenomen met 10 tegen 3 stemmen en 1 onthouding.

Art. 62

Amendement nr. 97 (*partim*) wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

Artikel 62 wordt aangenomen met 10 tegen 2 stemmen en 2 onthoudingen.

Art. 63 en 64

Amendement nr. 97 (*partim*) wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

De artikelen 63 en 64 wordt achtereenvolgens aangenomen met 11 stemmen tegen 1 en 2 onthoudingen.

Art. 65

Amendement nr. 97 (*partim*) wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

Artikel 65 wordt aangenomen met 9 tegen 4 stemmen en 1 onthouding.

Art. 66

Artikel 66 wordt aangenomen met 12 stemmen en 2 onthoudingen.

Art. 67

Amendement nr. 97 (*partim*) wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

Artikel 67 wordt aangenomen met 11 tegen 2 stemmen en 1 onthouding.

Les articles 54 à 60 sont successivement adoptés par 10 voix contre 2 et 2 abstentions.

Art. 61

L'amendement n° 97 (*partim*) est rejeté par 12 voix contre une et une abstention.

L'amendement n° 105 est rejeté par 12 voix contre une et une abstention.

L'article 61 est adopté par 10 voix contre 3 et une abstention.

Art. 62

L'amendement n° 97 (*partim*) est rejeté par 12 voix contre une et une abstention.

L'article 62 est adopté par 10 voix contre 2 et 2 abstentions.

Art. 63 et 64

L'amendement n° 97 (*partim*) est rejeté par 12 voix contre une et une abstention.

Les articles 63 et 64 sont successivement adoptés par 11 voix contre une et 2 abstentions.

Art. 65

L'amendement n° 97 (*partim*) est rejeté par 12 voix contre une et une abstention.

L'article 65 est adopté par 9 voix contre 4 et une abstention.

Art. 66

L'article 66 est adopté par 12 voix et 2 abstentions.

Art. 67

L'amendement n° 97 (*partim*) est rejeté par 12 voix contre une et une abstention.

L'article 67 est adopté par 11 voix contre 2 et une abstention.

Art. 68

Amendement nr. 97 (*partim*) wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

Artikel 65 wordt aangenomen met 11 stemmen tegen 1 en 2 onthoudingen.

Art. 69 tot 75

Amendement nr. 97 (*partim*) wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

De artikelen 69 tot 75 worden achtereenvolgens aangenomen met 10 tegen 2 stemmen en 2 onthoudingen.

Art. 76

Amendement nr. 97 (*partim*) wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

Amendement nr. 64 wordt aangenomen met 10 stemmen tegen 1 en 3 onthoudingen.

Artikel 76, aldus geamendeerd, wordt aangenomen met 10 tegen 2 stemmen en 2 onthoudingen.

Art. 77 tot 81

Amendement nr. 97 (*partim*) wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

De artikelen 77 en 78 worden achtereenvolgens aangenomen met 10 stemmen en 4 onthoudingen.

De artikelen 79 en 80 worden achtereenvolgens aangenomen met 11 stemmen tegen 1 en 2 onthoudingen.

Artikel 81 wordt aangenomen met 10 stemmen tegen 1 en 3 onthoudingen.

Art. 81/1 (*nieuw*)

Amendement nr. 65, dat een artikel 81/1 (*nieuw*) invoert, wordt aangenomen met 10 stemmen tegen 1 en 3 onthoudingen.

Art. 82 tot 84

Amendement nr. 97 (*partim*) wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

Art. 68

L'amendement n° 97 (*partim*) est rejeté par 12 voix contre une et une abstention.

L'article 65 est adopté par 11 voix contre une et 2 abstentions.

Art. 69 à 75

L'amendement n° 97 (*partim*) est rejeté par 12 voix contre une et une abstention.

Les articles 69 à 75 sont successivement adoptés par 10 voix contre 2 et 2 abstentions.

Art. 76

L'amendement n° 97 (*partim*) est rejeté par 12 voix contre une et une abstention.

L'amendement n° 64 est adopté par 10 voix contre une et 3 abstentions.

L'article 76, ainsi modifié, est adopté par 10 voix contre 2 et 2 abstentions.

Art. 77 à 81

L'amendement n° 97 (*partim*) est rejeté par 12 voix contre une et une abstention.

Les articles 77 et 78 sont successivement adoptés par 10 voix et 4 abstentions.

Les articles 79 et 80 sont successivement adoptés par 11 voix contre une et 2 abstentions.

L'article 81 est adopté par 10 voix contre une et 3 abstentions.

Art. 81/1 (*nouveau*)

L'amendement n° 65 tendant à insérer un article 81/1 est adopté par 10 voix contre une et 3 abstentions.

Articles 82 à 84

L'amendement n° 97 (*partim*) est rejeté par 12 voix contre une et une abstention.

De artikelen 82 tot 84 worden achtereenvolgens aangenomen met 10 stemmen tegen 1 en 3 onthoudingen.

Onderafdeling 2

Wijzigingen van de wet van 1 juni 2008 houdende de invoering van een belastingvermindering voor aandelen in ontwikkelingsfondsen voor microfinanciering in ontwikkelingslanden en houdende de vaststelling van de voorwaarden voor de erkenning als ontwikkelingsfonds

Art. 85 en 86

Amendement nr. 97 (*partim*) wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

De artikelen 85 en 86 worden achtereenvolgens aangenomen met 11 stemmen tegen 1 en 2 onthoudingen.

Onderafdeling 3

Inwerkingtreding

Art. 87

Amendement nr. 97 (*partim*) wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

De amendementen nrs. 66 en 67 worden achtereenvolgens aangenomen met 10 stemmen tegen 1 en 3 onthoudingen.

De amendementen nrs. 98 tot 100 worden achtereenvolgens verworpen met 12 tegen 2 stemmen.

Artikel 87, aldus geamendeerd, wordt aangenomen met 10 tegen 3 stemmen en 1 onthouding.

Les articles 82 à 84 sont successivement adoptés par 10 voix contre une et 3 abstentions.

Sous-section 2

Modifications de la loi du 1^{er} juin 2008 instaurant une réduction d'impôt pour les participations sous la forme d'actions dans des fonds de développement du microfinancement dans les pays en développement et fixant les conditions d'agrément en tant que fonds de développement

Art. 85 et 86

L'amendement n° 97 (*partim*) est rejeté par 12 voix contre une et une abstention.

Les articles 85 et 86 sont successivement adoptés par 11 voix contre une et 2 abstentions.

Sous-section 3

Entrée en vigueur

Art. 87

L'amendement n° 97 (*partim*) est rejeté par 12 voix contre une et une abstention.

Les amendements n° 66 et 67 sont successivement adoptés par 10 voix contre une et 3 abstentions.

Les amendements n° 98 à 100 sont successivement rejetés par 12 voix contre 2.

L'article 87, ainsi modifié, est adopté par 10 voix contre 3 et une abstention.

HOOFDSTUK 2

Procedure

Afdeling 1

Wijzigingen aangebracht aan de aanslagtermijnen en de onderzoektermijnen van het Wetboek van de inkomstenbelastingen 1992

Art. 87/1 en 87/2 (*nieuw*)

De artikelen 87/1 en 87/2 (*nieuw*) worden achtereenvolgens aangenomen met 11 tegen 3 stemmen.

Art. 88 en 89

Artikel 88 wordt aangenomen met 10 tegen 3 stemmen en 1 onthouding.

Artikel 89 wordt aangenomen met 11 tegen 3 stemmen.

Art. 89/1 (*nieuw*)

Artikel 89/1 (*nieuw*) wordt aangenomen met 11 tegen 3 stemmen.

Art. 90

Artikel 90 wordt aangenomen met 11 tegen 3 stemmen.

Afdeling 2

Wijzigingen aangebracht aan de verjaringstermijnen voor de vordering tot voldoening van de belasting in het Wetboek van de belasting over de toegevoegde waarde

Art. 90/1 (*nieuw*)

Artikel 90/1 (*nieuw*) wordt aangenomen met 11 tegen 3 stemmen.

Art. 91 en 92

De artikelen 91 en 92 worden achtereenvolgens aangenomen met 11 tegen 3 stemmen.

CHAPITRE 2

Procédure

Section 1^{re}

Modifications apportées aux délais d'imposition et d'investigation du Code des impôts sur les revenus 1992

Art. 87/1 et 87/2 (*nouveaux*)

Les articles 87/1 et 87/2 (*nouveaux*) sont successivement adoptés par 11 voix contre 3.

Art. 88 et 89

L'article 88 est adopté par 10 voix contre 3 et une abstention.

L'article 89 est adopté par 11 voix contre 3.

Art. 89/1 (*nouveau*)

L'article 89/1 (*nouveau*) est adopté par 11 voix contre 3.

Art. 90

L'article 90 est adopté par 11 voix contre 3.

Section 2

Modifications apportées aux délais de prescription de l'action en recouvrement de la taxe dans le Code de la taxe sur la valeur ajoutée

Art. 90/1 (*nouveau*)

L'article 90/1 (*nouveau*) est adopté par 11 voix contre 3.

Art. 91 et 92

Les articles 91 et 92 sont successivement adoptés par 11 voix contre 3.

Art. 93

Amendement nr. 68 wordt aangenomen met 10 stemmen tegen 1 en 3 onthoudingen.

Artikel 93, aldus geamendeerd, wordt aangenomen met 11 tegen 3 stemmen.

Art. 94 en 95

De artikelen 94 en 95 worden achtereenvolgens aangenomen met 11 tegen 3 stemmen.

HOOFDSTUK 3 (NIEUW)

Wijziging van het Wetboek diverse rechten en taksen, teneinde bepaalde ambtenaren toegang te geven tot het Centraal Aanspreekpunt van de Nationale Bank van België

Amendement nr. 77 wordt verworpen met 12 tegen 2 stemmen.

Art. 95/1 (*nieuw*)

De amendementen nrs. 78, 89 en 90 worden achtereenvolgens verworpen met 12 tegen 2 stemmen.

Artikel 95/1 (*nieuw*) wordt aangenomen met 12 tegen 2 stemmen.

Art. 95/2 (*nieuw*)

Amendement nr. 79 wordt verworpen met 12 tegen 2 stemmen.

Artikel 95/2 (*nieuw*) wordt aangenomen met 12 tegen 2 stemmen.

HOOFDSTUK 4 (NIEUW)

Wijziging van de wet van 3 augustus 2012 houdende bepalingen betreffende de verwerking van persoonsgegevens door de Federale Overheidsdienst Financiën in het kader van zijn opdrachten

Art. 95/3 (*nieuw*)

Amendement nr. 81 wordt verworpen met 12 tegen 2 stemmen.

Art. 93

L'amendement n° 68 est adopté par 10 voix contre une et 3 abstentions.

L'article 93, ainsi modifié, est adopté par 11 voix contre 3.

Art. 94 et 95

Les articles 94 et 95 sont successivement adoptés par 11 voix contre 3.

CHAPITRE 3 (NOUVEAU)

Modification du Code des droits et taxes divers visant à octroyer à certains fonctionnaires l'accès au point de contact central de la Banque Nationale de Belgique

L'amendement n° 77 est rejeté par 12 voix contre 2.

Art. 95/1 (*nouveau*)

Les amendements n° s 78, 89 et 90 sont successivement rejetés par 12 voix contre 2.

L'article 95/1 (*nouveau*) est adopté par 12 voix contre 2.

Art. 95/2 (*nouveau*)

L'amendement n° 79 est rejeté par 12 voix contre 2.

L'article 95/2 (*nouveau*) est adopté par 12 voix contre 2.

CHAPITRE 4 (NOUVEAU)

Modification de la loi du 3 août 2012 portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions

Art. 95/3 (*nouveau*)

L'amendement n° 81 est rejeté par 12 voix contre 2.

De amendementen nrs. 88 en 106 worden achter-eenvolgens verworpen met 12 stemmen tegen 1 en 1 onthouding.

Amendement nr. 101 wordt verworpen met 11 tegen 2 stemmen en 1 onthouding.

Artikel 95/3 (*nieuw*) wordt aangenomen met 12 tegen 2 stemmen.

HOOFDSTUK 5 (*NIEUW*)

Wijziging van de wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van rekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest

Amendement nr. 82 wordt verworpen met 12 tegen 2 stemmen.

Art. 95/4 (*nieuw*)

Amendement nr. 83 wordt verworpen met 12 tegen 2 stemmen.

Artikel 95/4 (*nieuw*) wordt aangenomen met 12 tegen 2 stemmen.

Art. 95/5 (*nieuw*)

Amendement nr. 84 wordt verworpen met 12 tegen 2 stemmen.

Artikel 95/5 (*nieuw*) wordt aangenomen met 12 tegen 2 stemmen.

Art. 95/6 (*nieuw*)

Amendement nr. 85 wordt verworpen met 12 tegen 2 stemmen.

Artikel 95/6 (*nieuw*) wordt aangenomen met 12 tegen 2 stemmen.

Art. 95/7 (*nieuw*)

Amendement nr. 86 wordt verworpen met 12 tegen 2 stemmen.

Les amendements n° 88 et 106 sont successivement rejetés par 12 voix contre une et une abstention.

L'amendement n° 101 est rejeté par 11 voix contre 2 et une abstention.

L'article 95/3 (*nouveau*) est adopté par 12 voix contre 2.

CHAPITRE 5 (*NOUVEAU*)

Modifications de la loi du 8 juillet 2018 portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt

L'amendement n° 82 est rejeté par 12 voix contre 2.

Art. 95/4 (*nouveau*)

L'amendement n° 83 est rejeté par 12 voix contre 2.

L'article 95/4 (*nouveau*) est adopté par 12 voix contre 2.

Art. 95/5 (*nouveau*)

L'amendement n° 84 est rejeté par 12 voix contre 2.

L'article 95/5 (*nouveau*) est adopté par 12 voix contre 2.

Art. 95/6 (*nouveau*)

L'amendement n° 85 est rejeté par 12 voix contre 2.

L'article 95/6 (*nouveau*) est adopté par 12 voix contre 2.

Art. 95/7 (*nouveau*)

L'amendement n° 86 est rejeté par 12 voix contre 2.

Artikel 95/7 (*nieuw*) wordt aangenomen met 12 tegen 2 stemmen.

Art. 95/8 (*nieuw*)

Amendement nr. 87 wordt verworpen met 12 tegen 2 stemmen.

Artikel 95/8 (*nieuw*) wordt aangenomen met 12 tegen 2 stemmen.

Art. 95/8/1 (*nieuw*)

Amendement nr. 107, dat een artikel 95/8/1 beoogt in te voegen, wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

Art. 95/8/2 (*nieuw*)

Amendement nr. 108, dat een artikel 95/8/2 beoogt in te voegen, wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

HOOFDSTUK 6 (*NIEUW*)

Maaltijdcheques

Amendement nr. 72, dat het opschrift van hoofdstuk 6 (*nieuw*) invoegt, wordt aangenomen met 12 stemmen tegen 1 en 1 onthouding.

Amendement nr. 69 (*partim*) wordt verworpen met 10 tegen 2 stemmen en 2 onthoudingen.

Art. 95/9 (*nieuw*)

Amendement nr. 73, dat artikel 95/9 (*nieuw*) invoegt, wordt aangenomen met 12 stemmen tegen 1 en 1 onthouding.

Amendement nr. 69 (*partim*) wordt verworpen met 10 tegen 2 stemmen en 2 onthoudingen.

Art. 95/10 (*nieuw*)

Amendement nr. 74, dat artikel 95/10 (*nieuw*) invoegt, wordt aangenomen met 11 tegen 2 stemmen en 1 onthouding.

L'article 95/7 (*nouveau*) est adopté par 12 voix contre 2.

Art. 95/8 (*nouveau*)

L'amendement n° 87 est rejeté par 12 voix contre 2.

L'article 95/8 (*nouveau*) est adopté par 12 voix contre 2.

Art. 95/8/1 (*nouveau*)

L'amendement n° 107 tendant à insérer un article 95/8/1 est rejeté par 12 voix contre une et une abstention.

Art. 95/8/2 (*nouveau*)

L'amendement n° 108 tendant à insérer un article 95/8/2 est rejeté par 12 voix contre une et une abstention.

CHAPITRE 6 (*NOUVEAU*)

Titres-repas

L'amendement n° 72 tendant à insérer un chapitre 6 est adopté par 12 voix contre une et une abstention.

L'amendement n° 69 (*partim*) est rejeté par 10 voix contre 2 et 2 abstentions.

Art. 95/9 (*nouveau*)

L'amendement n° 73 tendant à insérer un article 95/9 (*nouveau*) est adopté par 12 voix contre une et une abstention.

L'amendement n° 69 (*partim*) est rejeté par 10 voix contre 2 et 2 abstentions.

Art. 95/10 (*nouveau*)

L'amendement n° 74 tendant à insérer un 95/10 est adopté par 11 voix contre 2 et une abstention.

Amendement nr. 70 wordt verworpen met 10 stemmen tegen 1 en 3 onthoudingen.

Art. 95/11 (*nieuw*)

Amendement nr. 75, dat artikel 95/11 (*nieuw*) invoegt, wordt aangenomen met 13 stemmen tegen 1 en 1 onthouding.

Amendement nr. 71 wordt verworpen met 12 tegen 2 stemmen.

Art. 95/12 (*nieuw*)

Amendement nr. 76, dat artikel 95/12 (*nieuw*) invoegt, wordt verworpen met 12 stemmen tegen 1 en 1 onthouding.

*
* *

Het geheel van de naar de commissie verwezen artikelen van het wetsontwerp nr. 963, aldus geamendeerd, wordt bij naamstemming en met inbegrip van een reeks taalkundige en wetgevingstechnische verbeteringen, aangenomen met 9 tegen 4 stemmen en 1 onthouding.

Resultaat van de naamstemming:

Hebben voorgestemd:

N-VA: Wim Van der Donckt, Steven Vandeput, Charlotte Verkeyn;

MR: Mathieu Michel, Benoît Piedboeuf;

Les Engagés: Xavier Dubois, Stéphane Lasseaux;

Vooruit: Niels Tas;

cd&v: Nawal Farih.

Hebben tegengestemd:

PS: Hugues Bayet;

PVDA-PTB: Kemal Bilmez;

Ecolo-Groen: Dieter Vanbesien;

Open Vld: Vincent Van Quickenborne.

L'amendement n° 70 est rejeté par 10 voix contre une et 3 abstentions.

Art. 95/11 (*nouveau*)

L'amendement n° 75 tendant à insérer un article 95/11 est adopté par 13 voix contre une et une abstention.

L'amendement n° 71 est rejeté par 12 voix contre 2.

Art. 95/12 (*nouveau*)

L'amendement n° 76 tendant à insérer un article 95/12 est rejeté par 12 voix contre une et une abstention.

*
* *

L'ensemble des articles du projet de loi n° 963 renvoyés à la commission, tels qu'ils ont été modifiés, en ce compris une série de modifications d'ordre linguistique et légistique, est adopté par vote nominatif par 9 voix contre 4 et une abstention.

Résultat du vote nominatif:

Ont voté pour:

N-VA: Wim Van der Donckt, Steven Vandeput, Charlotte Verkeyn;

MR: Mathieu Michel, Benoît Piedboeuf,

Les Engagés: Xavier Dubois, Stéphane Lasseaux,

Vooruit: Niels Tas;

cd&v: Nawal Farih.

Ont voté contre:

PS: Hugues Bayet;

PVDA-PTB: Kemal Bilmez;

Ecolo-Groen: Dieter Vanbesien;

Open Vld: Vincent Van Quickenborne.

Heeft zich onthouden:

VB: Lode Vereeck.

Dit verslag werd goedgekeurd met 10 stemmen en 4 onthoudingen.

De rapporteur,

De voorzitter,

Vincent Van Quickenborne

Steven Vandeput

Lijst met bepalingen die een uitvoeringsmaatregel vergen (art. 78.2 van het Reglement):

— art. 23, 26, 86 en 102.

S'est abstenu:

VB: Lode Vereeck.

Le présent rapport a été approuvé par 10 voix et 4 abstentions.

Le rapporteur,

Le président,

Vincent Van Quickenborne

Steven Vandeput

Dispositions nécessitent une mesure d'exécution (art. 78.2 du Règlement):

— art. 23, 26, 86 et 102.

NOTA TER ATTENTIE VAN DE COMMISSIE VOOR FINANCIËN EN BEGROTING

Betreft: Wetgevingstechnische nota betreffende de in eerste lezing aangenomen artikelen van het wetsontwerp houdende diverse bepalingen (*partim* Financiën: art. 1 tot 95/8) (DOC 56-0963/020).

ALGEMENE OPMERKINGEN

1. In titel 2, hoofdstuk 1, afdeling 11, onderafdeling 1, van het wetsontwerp worden verschillende artikelen van het Wetboek van de inkomstenbelastingen 1992 (hierna: "WIB 92") opgeheven. Het staat aan de commissie de verwijzingen naar die opgeheven artikelen te verifiëren en aan te passen, niet alleen in het WIB 92 maar ook in andere wetten. Ter illustratie kan op niet-exhaustieve wijze verwezen worden naar de volgende artikelen die niet gewijzigd worden door het wetsontwerp maar die wel een verwijzing bevatten naar een van de opgeheven artikelen van het WIB 92:
 - artikel 145²⁶, § 3, derde lid, 1°, WIB 92 dat verwijst naar artikel 145³² WIB 92 dat opgeheven wordt bij artikel 64 van het wetsontwerp;
 - artikel 145²⁷, § 2, vijfde lid, 1°, WIB 92 dat verwijst naar het opgeheven artikel 145³² WIB 92;
 - artikel 175 WIB 92 dat verwijst naar het opgeheven artikel 145³², § 2, WIB 92;
 - artikel 531 WIB 92 dat verwijst naar artikel 67, § 4, WIB 92 dat opgeheven wordt bij artikel 55 van het wetsontwerp;
 - artikel 10, § 1, tweede lid, van de wet van 17 maart 2019 'betreffende de invoering van een mobiliteitsbudget' dat verwijst naar artikel 145²⁸ WIB 92 dat opgeheven wordt bij artikel 62 van het wetsontwerp.

Bij de aanpassing van de verwijzingen naar de opgeheven artikelen van het WIB 92 zal de commissie rekening dienen te houden met de verschillende data waarop de opheffingsbepalingen in werking treden, zoals bepaald in artikel 87 van het wetsontwerp.

2. De artikelen 85 en 86 van het wetsontwerp heffen respectievelijk de artikelen 2 en 3 op van de wet van 1 juni 2008 'houdende de invoering van een belastingsvermindering voor aandelen in ontwikkelingsfondsen voor microfinanciering in ontwikkelingslanden en houdende de vaststelling van de voorwaarden voor de erkenning als ontwikkelingsfonds'. Het staat aan de commissie de verwijzingen naar die opgeheven artikelen in andere wetten te verifiëren en aan te passen, daarbij rekening houdend met het feit dat de artikelen 85 en 86 van het wetsontwerp krachtens artikel 87, zevende lid, van het wetsontwerp pas in werking treden op 1 januari 2031.

Ter illustratie kan op niet-exhaustieve wijze verwezen worden naar artikel 180, § 2, 2°, van de wet van 19 april 2014 'betreffende de alternatieve instellingen voor collectieve belegging en hun beheerders' dat verwijst naar "de ontwikkelingsfondsen bedoeld in artikel 2, 1° van de wet van 1 juni 2008 (...)".

BIJZONDERE OPMERKINGEN BIJ DE ARTIKELN**Art. 41**

3. Men voege in artikel 41 van het wetsontwerp een bepaling onder c)/1 in, luidende:

"c)/1. in paragraaf 3, in het vroegere vierde lid, dat het vijfde lid wordt, worden de woorden "overeenkomstig het derde lid, 2^o" vervangen door de woorden "overeenkomstig het vierde lid, 2^o";"

/

"c)/1. dans le paragraphe 3, dans l'alinéa 4 ancien, devenant l'alinéa 5, les mots "conformément à l'alinéa 3, 2^o" sont remplacés par les mots "conformément à l'alinéa 4, 2^o";".

(Aanpassing van de kruisverwijzing in een van de onderverdelingen van paragraaf 3 van artikel 178 WIB 92 ten gevolge van de invoeging, bij de bepaling onder c), van een lid, tussen het tweede en het derde lid, in die paragraaf.)

Art. 41/1

4. Men voege in het wetsontwerp een nieuw artikel 41/1 in, luidende:

"Art. 41/1. In artikel 70 van de wet van 5 juli 2022 houdende diverse fiscale bepalingen worden de woorden "In artikel 178, § 3, derde lid, van hetzelfde Wetboek" vervangen door de woorden "In artikel 178, § 3, vierde lid, van hetzelfde Wetboek"."

/

"Art. 41/1. Dans l'article 70 de la loi du 5 juillet 2022 portant des dispositions fiscales diverses, les mots "Dans l'article 178, § 3, alinéa 3, du même Code" sont remplacés par les mots "Dans l'article 178, § 3, alinéa 4, du même Code"."

(Bij artikel 70 van de wet van 5 juli 2022 'houdende diverse fiscale bepalingen', dat krachtens artikel 71, zeventiende lid, van dezelfde wet van toepassing is vanaf aanslagjaar 2028, wordt de inleidende zin van artikel 178, § 3, derde lid, WIB 92 gewijzigd. Ten gevolge van de wijziging aangebracht door artikel 41, c), van het wetsontwerp, dat krachtens artikel 42 van het wetsontwerp al van toepassing is vanaf aanslagjaar 2026, wordt het derde lid van artikel 178, § 3, WIB 92 echter het vierde lid. Het voorgestelde nieuwe artikel 41/1 strekt ertoe het onderdeel van artikel 178, § 3, WIB 92 waarin de door artikel 70 van de wet van 5 juli 2022 beoogde wijziging aangebracht moet worden aan te passen aan de door artikel 41, c), van het wetsontwerp beoogde wijziging.)

Indien de commissie gevolg geeft aan deze opmerking, dan vervange men in de inleidende zin van artikel 43 van het wetsontwerp de woorden "van hetzelfde Wetboek" / "du même Code" door de woorden "van het Wetboek van de inkomstenbelastingen 1992" / "du Code des impôts sur les revenus 1992".

Art. 60

5. Bij artikel 51 van het wetsontwerp wordt artikel 38, § 1, eerste lid, 17°, WIB 92 opgeheven en die opheffing heeft krachtens artikel 87, eerste lid, van het wetsontwerp uitwerking met ingang van 30 september 2025. Bij artikel 60, 1°, van het wetsontwerp wordt in artikel 129/1, eerste lid, WIB 92 de verwijzing naar artikel 38, § 1, eerste lid, 17°, WIB 92 opgeheven waarbij die opheffing krachtens artikel 87, vijfde lid, van het wetsontwerp van toepassing is vanaf aanslagjaar 2027. Dat betekent dat tot aanslagjaar 2027 artikel 129/1, eerste lid, WIB 92 zal verwijzen naar het bedrag vermeld in artikel 38, § 1, eerste lid, 17°, WIB 92 terwijl die bepaling al met ingang van 30 september 2025 opgeheven is. De vraag rijst dan ook of in artikel 129/1, eerste lid, WIB 92 de verwijzing naar artikel 38, § 1, eerste lid, 17°, WIB 92 in eerste instantie niet vervangen moet worden door een verwijzing naar "artikel 38, § 1, eerste lid, 17°, zoals het bestond alvorens het werd opgeheven bij artikel 51 van de wet van ... houdende diverse bepalingen" alvorens de verwijzing definitief op te heffen vanaf aanslagjaar 2027.

Art. 76

6. In de bepaling onder a), die wijzigingen aanbrengt in de inleidende zin van artikel 243/1 WIB 92, worden de woorden "¹⁴⁵²⁶, ¹⁴⁵²⁸, ¹⁴⁵³² tot ¹⁴⁵³⁵, ¹⁴⁵⁴⁸," vervangen door de woorden "¹⁴⁵²⁶, ¹⁴⁵³³, ¹⁴⁵³⁵,". Die wijzigingsbepaling loopt op twee punten mank:
- 1° in de inleidende zin van artikel 243/1 WIB 92 is er eigenlijk sprake van de woorden "¹⁴⁵²⁶ tot ¹⁴⁵²⁸"¹, in plaats van de woorden "¹⁴⁵²⁶, ¹⁴⁵²⁸", zodat de inleidende zin thans ook verwijst naar artikel ¹⁴⁵^{26/1} WIB 92, dat opgeheven wordt bij artikel 61 van het wetsontwerp, en naar artikel ¹⁴⁵²⁷ WIB 92, dat niet opgeheven wordt door het wetsontwerp;
 - 2° de inleidende zin van artikel 243/1 WIB 92 verwijst thans ook naar artikel ¹⁴⁵⁵⁰ WIB 92² dat opgeheven wordt bij artikel 69 van het wetsontwerp.

De vraag rijst dan ook of in de inleidende zin van artikel 243/1 WIB 92 de woorden "¹⁴⁵²⁶ tot ¹⁴⁵²⁸, ¹⁴⁵³² tot ¹⁴⁵³⁵, ¹⁴⁵⁴⁸, ¹⁴⁵⁵⁰," niet vervangen moeten worden door de woorden "¹⁴⁵²⁶, ¹⁴⁵²⁷, ¹⁴⁵³³, ¹⁴⁵³⁵,". Op die manier wordt enerzijds de verwijzing naar de opgeheven artikelen ¹⁴⁵^{26/1} en ¹⁴⁵⁵⁰ WIB 92 weggelaten terwijl anderzijds de verwijzing naar artikel ¹⁴⁵²⁷ WIB 92, dat niet opgeheven wordt door het wetsontwerp, behouden blijft. De voorgestelde wijziging is trouwens niet in strijd met de in artikel 87 van het wetsontwerp bepaalde inwerkingtreding van de betrokken bepalingen aangezien zowel de opheffing van de artikelen ¹⁴⁵^{26/1} en ¹⁴⁵⁵⁰ WIB 92 als artikel 76, a), van het wetsontwerp krachtens artikel 87, vierde lid, van het wetsontwerp van toepassing zijn vanaf aanslagjaar 2026.

Het staat aan de commissie artikel 76, a), van het wetsontwerp opnieuw te onderzoeken.

7. In de bepaling onder c), die wijzigingen aanbrengt in artikel 243/1, 4°, WIB 92, worden de woorden "¹⁴⁵^{26/1}, §§ 1 en 2, ¹⁴⁵²⁷, §§ 1 tot 3, ¹⁴⁵²⁸, ¹⁴⁵³², § 1, ¹⁴⁵³³ tot ¹⁴⁵³⁵, ¹⁴⁵⁴⁸," vervangen door de woorden "¹⁴⁵²⁷, §§ 1 tot 3, ¹⁴⁵³³, ¹⁴⁵³⁵,". Aangezien artikel 243/1, 4°, WIB 92 thans ook verwijst naar artikel ¹⁴⁵⁵⁰ WIB 92³, dat opgeheven wordt bij artikel 69 van het wetsontwerp, rijst de vraag of

¹ Bij artikel 35, 1°, van de wet van 26 maart 2018 'betreffende de versterking van de economische groei en de sociale cohesie' werden in de inleidende zin van artikel 243/1 WIB 92 de woorden "¹⁴⁵²⁶, ¹⁴⁵²⁸," vervangen door de woorden "¹⁴⁵²⁶ tot ¹⁴⁵²⁸,".

² Bij artikel 19, 1°, van de wet van 25 november 2021 'houdende fiscale en sociale vergroening van de mobiliteit' werden in de inleidende zin van artikel 243/1 WIB 92 de woorden "¹⁴⁵⁴⁸, 146 tot 154bis" vervangen door de woorden "¹⁴⁵⁴⁸, ¹⁴⁵⁵⁰, 146 tot 154bis".

³ Bij artikel 19, 2°, van de wet van 25 november 2021 'houdende fiscale en sociale vergroening van de mobiliteit' werden in artikel 243/1, 4°, WIB 92 de woorden "¹⁴⁵⁴⁸, 154bis" vervangen door de woorden "¹⁴⁵⁴⁸, ¹⁴⁵⁵⁰, 154bis".

in artikel 243/1, 4°, WIB 92 niet eerder de woorden "¹⁴⁵26/1, §§ 1 en 2, ¹⁴⁵27, §§ 1 tot 3, ¹⁴⁵28, ¹⁴⁵32, § 1, ¹⁴⁵33 tot ¹⁴⁵35, ¹⁴⁵48, ¹⁴⁵50" vervangen moeten worden door de woorden "¹⁴⁵27, §§ 1 tot 3, ¹⁴⁵33, ¹⁴⁵35". De voorgestelde wijziging is trouwens niet in strijd met de in artikel 87 van het wetsontwerp bepaalde inwerkingtreding van de betrokken bepalingen aangezien zowel de opheffing van artikel 145⁵⁰ WIB 92 als artikel 76, c), van het wetsontwerp krachtens artikel 87, vierde lid, van het wetsontwerp van toepassing zijn vanaf aanslagjaar 2026.

Art. 87

8. Artikel 87 van het wetsontwerp bepaalt de inwerkingtreding van alle artikelen opgenomen in titel 2, hoofdstuk 1, afdeling 11, onderafdelingen 1 en 2, van het wetsontwerp, te weten de artikelen 51 tot 86. Voor een artikel, namelijk artikel 70 van het wetsontwerp, wordt de inwerkingtreding echter niet geregeld. Dat laatste artikel heft in artikel 171 WIB 92, in de inleidende zin van de bepaling onder 6°, de verwijzing op naar de opgeheven artikelen ¹⁴⁵26/1, ¹⁴⁵28, ¹⁴⁵32, ¹⁴⁵34, ¹⁴⁵48, ¹⁴⁵49 en ¹⁴⁵50 van hetzelfde Wetboek.

Aangezien de artikelen 61, 62 en 66 tot 69 van het wetsontwerp, die respectievelijk de artikelen ¹⁴⁵26/1, ¹⁴⁵28, ¹⁴⁵34, ¹⁴⁵48, ¹⁴⁵49 en ¹⁴⁵50 WIB 92 opheffen, allen van toepassing zijn vanaf aanslagjaar 2026 en de in artikel ¹⁴⁵32 WIB 92 bedoelde belastingvermindering niet meer verleend wordt vanaf aanslagjaar 2026⁴, rijst de vraag of artikel 87, vierde lid, van het wetsontwerp niet aangevuld moet worden met een verwijzing naar artikel 70 van het wetsontwerp.

Art. 92

9. Waar het huidige artikel 84^{ter} van het Wetboek van de belasting over de toegevoegde waarde (hierna: "BTW-Wetboek") gewag maakt van "*aanwijzingen van fraude*" / "*les indices de fraude*", verwijst het ontworpen artikel 84^{ter} van het BTW-Wetboek in het Nederlands naar "*aanwijzingen van fraude*" en in het Frans naar "*les indices de fraude fiscale*". De vraag rijst welke taalversie correct is en, meer fundamenteel, welke fraude bedoeld wordt.⁵
Dezelfde opmerking geldt voor artikel 93 van het wetsontwerp (toekomstige versie van artikel 84^{ter} van het BTW-Wetboek.)

Art. 93

10. Artikel 84^{ter} van het BTW-Wetboek wordt vervangen bij artikel 92 van het wetsontwerp dat in werking zal treden op de tiende dag na publicatie van de aan te nemen wet in het *Belgisch Staatsblad*. Artikel 84^{ter} van het BTW-Wetboek wordt echter ook vervangen bij artikel 56 van de wet van 12 mei 2024 'tot digitalisatie van de relaties tussen de Federale Overheidsdienst Financiën, de burgers, de bedrijven, de rechtspersonen en bepaalde derden en tot opheffing van de wet van 26 januari 2021 betreffende de dematerialisatie van de relaties tussen de Federale Overheidsdienst Financiën, de burgers, rechtspersonen en bepaalde derden en tot wijziging van diverse fiscale wetboeken en wetten' dat in werking zal treden op een datum te bepalen door de Koning en ten laatste op 1 januari 2028⁶. Hierdoor dreigt de bij artikel 92 van het wetsontwerp beoogde wijziging ongedaan gemaakt te worden op het moment dat artikel

⁴ Zie de toelichting bij de artikelen 63 en 64 van het wetsontwerp: DOC 56-0963/001, blz. 36-37.

⁵ Zie de toelichting bij artikel 92 van het wetsontwerp: DOC 56-0963/001, blz. 41: "*Het is momenteel voorzien dat deze kennisgeving voorafgaandelijk aan de rechtzetting en op nauwkeurige wijze aan de betrokken persoon vermeldt de aanwijzingen van fiscale fraude die tegenover hem bestaan.*" (eigen onderlijning).

⁶ Art. 222 van de wet van 12 mei 2024.

56 van de wet van 12 mei 2024 in werking treedt. Om dit te vermijden werd ervoor gekozen om in artikel 93 van het wetsontwerp artikel 84ter van het BTW-Wetboek opnieuw te vervangen, rekening houdende met zowel de bij artikel 92 van het wetsontwerp als de bij artikel 56 van de wet van 12 mei 2024 beoogde wijziging, waarbij artikel 93 van het wetsontwerp op dezelfde datum in werking zal treden als artikel 56 van de wet van 12 mei 2024.⁷ De inleidende zin van artikel 93 van het wetsontwerp, zoals hij thans is opgesteld, neemt echter niet het risico weg, nu artikel 56 van de wet van 12 mei 2024 niet opgeheven wordt, dat er op de vastgestelde datum van inwerkingtreding onduidelijkheid bestaat of de bij artikel 93 van het wetsontwerp dan wel de bij artikel 56 van de wet van 12 mei 2024 beoogde vervanging eerst doorgevoerd moet worden. Dit risico kan vermeden worden door:

- ofwel artikel 56 van de wet van 12 mei 2024 te wijzigen om rekening te houden met de door artikel 92 van het wetsontwerp beoogde wijziging in plaats van opnieuw rechtstreeks in te grijpen in artikel 84ter van het BTW-Wetboek;
- ofwel artikel 56 van de wet van 12 mei 2024 op te heffen waarbij die opheffing uiterlijk de dag vóór de datum van inwerkingtreding van dat artikel in werking moet treden. In dat geval vervange men in de inleidende zin van artikel 93 van het wetsontwerp de woorden "vervangen bij de wet van 23 november 2023" / "remplacé par la loi du 23 novembre 2023" door de woorden "vervangen bij artikel 92" / "remplacé par l'article 92";
- ofwel uit de inleidende zin van artikel 93 van het wetsontwerp duidelijk te laten blijken dat er rekening werd gehouden met de nog niet in werking getreden wijzigingsbepaling.⁸

Indien de commissie kiest voor de laatste oplossing, dan vervange men de inleidende zin van artikel 93 van het wetsontwerp als volgt: "*Artikel 84ter van hetzelfde Wetboek, ingevoegd bij de wet van 15 maart 1999, vervangen bij artikel 92 en zoals vervangen bij de wet van 12 mei 2024, wordt vervangen als volgt:*" / "*L'article 84ter du même Code, inséré par la loi du 15 mars 1999, remplacé par l'article 92 et tel que remplacé par la loi du 12 mai 2024, est remplacé par ce qui suit:*".

LOUTER VORMELIJKE VERBETERINGEN EN TAALKUNDIGE CORRECTIES

Art. 2

11. In de Franse tekst van de bepaling onder 2° vervange men de woorden "*et les mots 'les intérêts et' sont abrogés;*" door de woorden "*et les mots 'les intérêts et redevances visés à l'alinéa 1^{er}, ne sont déductibles que lorsqu'ils ont été payés pendant' sont remplacés par les mots 'les redevances visées à l'alinéa 1^{er}, ne sont déductibles que lorsqu'elles ont été payées pendant';*".
(Taalkundige verbetering.)

Art. 14

12. In het tweede lid vervange men de woorden "*levensverzekeringscontracten en leningsovereenkomsten*" / "*contrats d'assurance-vie conclus individuellement et des emprunts*" door de woorden "*levensverzekeringscontracten en hypothecaire leningsovereenkomsten*" / "*contrats d'assurance-vie conclus individuellement et des emprunts hypothécaires*".
(De terminologie van de bepaling wordt in overeenstemming gebracht met die van artikel 323/1, § 1, eerste lid, WIB 92, zoals gewijzigd bij artikel 8, 1°, van het wetsontwerp.)

⁷ Zie de toelichting bij artikel 93 van het wetsontwerp: DOC 56-0963/001, blz. 41.

⁸ Raad van State, *Beginselen van de wetgevingstechniek. Handleiding voor het opstellen van wetgevende en reglementaire teksten*, 2008, blz. 84, nrs. 130-131.

Art. 23

13. In de bepaling onder 8°, in het ontworpen artikel 66, § 4, WIB 92, vervange men de woorden "*In afwijking van de paragrafen 1 en 1/1 van dit artikel en artikel 550*" / "*Par dérogation aux paragraphes 1^{er} et 1^{er}/1 du présent article et à l'article 550*" door de woorden "*In afwijking van de paragrafen 1 en 1/1 en artikel 550*" / "*Par dérogation aux paragraphes 1^{er} et 1^{er}/1 et à l'article 550*". (Wetgevingstechnische verbetering: bij een verwijzing binnen eenzelfde indeling van een tekst hoeft niet herhaald te worden dat het gaat om dezelfde indeling.⁹)

Art. 41

14. In de Nederlandse tekst van de bepaling onder c), in het ontworpen artikel 178, § 3, derde lid, WIB 92, vervange men de woorden "*indexcijfers van het jaar van de inkomsten voorafgaat*" door de woorden "*indexcijfers van het jaar dat het jaar van de inkomsten voorafgaat*". (Overeenstemming met de Franse tekst: "... des indices des prix de l'année qui précède celle des revenus ...".)

Art. 43

15. In de Franse tekst van het ontworpen artikel 206/3, § 1, tweede lid, tweede streepje, WIB 92 vervange men de woorden "*avant la reprise du transfert intra-groupe repris dans la base*" door de woorden "*avant la reprise du transfert intra-groupe dans la base*". (Het woord "*repris*" werd weggelaten omdat het dubbel gebruik vormt met de woorden "*la reprise*" en omdat het woord geen tegenhanger heeft in de Nederlandse tekst.)

Art. 89/1 (nieuw)

16. In de Nederlandse tekst van het ontworpen artikel 354/1 WIB 92 vervange men in de inleidende zin de woorden "*De bijkomende termijn*" door de woorden "*De aanvullende termijn*". (Overeenstemming van de bewoordingen van de ontworpen bepaling met die van het ontworpen artikel 333, derde lid, WIB 92 [art. 88 van het wetsontwerp] en met die van de inleidende zin van het huidige artikel 354/1 WIB 92.)

Art. 95/1 (nieuw)

17. In het ontworpen artikel 201/9/7, § 1, eerste lid, van het Wetboek diverse rechten en taken vervange men de woorden "*in artikel 4, 1°/1 van de voornoemde wet*" / "*à l'article 4, 1°/1 de la loi*" door de woorden "*in artikel 4, eerste lid, 1°/1, van de voornoemde wet*" / "*à l'article 4, alinéa 1^{er}, 1°/1, de la loi*". (Precisering van de verwijzing.)

Art. 95/2 (nieuw)

18. Men vervange de woorden "*de dag bepaald in artikel 95/8 van deze wet*" / "*à la date visée à l'article 95/8 de la présente loi*" door de woorden "*de datum bepaald in artikel 95/8, eerste lid*" / "*à la date visée à l'article 95/8, alinéa 1^{er}*".

⁹ Raad van State, o.c., blz. 59, nr. 72, a).

(Precisering van de verwijzing en harmonisatie van de beide taalversies. + Wetgevingstechnische verbetering: bij een verwijzing binnen dezelfde tekst hoeft niet herhaald te worden dat het gaat om dezelfde tekst.¹⁰)

VERBETERINGEN BETREFFENDE DE INLEIDENDE ZINNEN VAN DE ARTIKELN

- Art. 2: *"In artikel 14 van het Wetboek van de inkomstenbelastingen 1992, vervangen bij de wet van 6 juli 1994 en laatstelijk gewijzigd bij de wet van 21 januari 2022, worden" / "À l'article 14 du Code des impôts sur les revenus 1992, remplacé par la loi du 6 juillet 1994 et modifié en dernier lieu par la loi du 21 janvier 2022, les modifications".*
- Art. 4, b): *"in de bepaling onder 6° wordt in de inleidende zin het nummer" / "au 6°, dans la phrase liminaire, le nombre".*
- Art. 21: *"In artikel 36, § 2, negende lid, van hetzelfde Wetboek, ingevoegd bij de wet van 25 december 2017, zelf gewijzigd bij de wet van 2 mei 2019, en gewijzigd bij de wet van 27 juni 2021, worden" / "Dans l'article 36, § 2, alinéa 9, du même Code, inséré par la loi du 25 décembre 2017, elle-même modifiée par la loi du 2 mai 2019, et modifié par la loi du 27 juin 2021, les mots".*
- Art. 22, 5°: *"paragraaf 1/1, tweede lid, vervangen bij de bepaling onder 3° en gewijzigd bij de bepaling onder 4°, wordt aangevuld" / "le paragraphe 1^{er}/1, alinéa 2, remplacé par le 3° et modifié par le 4°, est complété".*
- Art. 29: *"In artikel 72 van hetzelfde Wetboek, gewijzigd bij het koninklijk besluit van 20 juli 2000, zelf gewijzigd bij het koninklijk besluit van 13 juli 2001, wordt" / "Dans l'article 72 du même Code, modifié par l'arrêté royal du 20 juillet 2000, lui-même modifié par l'arrêté royal du 13 juillet 2001, l'alinéa 2".*
- Art. 38: *"In artikel 145 van hetzelfde Wetboek, vervangen bij de wet van 18 december 2016 en gewijzigd bij de wet van 17 maart 2019, worden" / "À l'article 145 du même Code, remplacé par la loi du 18 décembre 2016 et modifié par la loi du 17 mars 2019, les".*
- Art. 46: *"Artikel 246, eerste lid, van hetzelfde Wetboek, laatstelijk gewijzigd bij de wet van 18 juli 2025, wordt aangevuld" / "L'article 246, alinéa 1^{er}, du même Code, modifié en dernier lieu par la loi du 18 juillet 2025, est complété".*
- Art. 49: *"In artikel 289bis, § 1, eerste lid, inleidende zin, van hetzelfde Wetboek, ingevoegd bij de wet van 20 december 1995 en vervangen bij de wet van 8 mei 2014, worden" / "Dans l'article 289bis, § 1^{er}, alinéa 1^{er}, phrase liminaire, du même Code, inséré par la loi du 20 décembre 1995 et remplacé par la loi du 8 mai 2014, les".*

¹⁰ Raad van State, o.c., blz. 59, nr. 72, a).

- Art. 58: *"In titel II, hoofdstuk II, afdeling 4, onderafdeling 3, B, van hetzelfde Wetboek, wordt het onderdeel "1^oter Bijkomend personeel", dat het artikel 67ter bevat, ingevoegd bij de wet van 8 juni 2008 en gewijzigd bij artikel 57, opgeheven." / "Dans le titre II, chapitre II, section 4, sous-section 3, B, du même Code, la partie "1^oter Personnel supplémentaire", qui comprend l'article 67ter, insérée par la loi du 8 juin 2008 et modifiée par l'article 57, est abrogée."*
- Art. 63: *"In artikel 145³² van hetzelfde Wetboek, ingevoegd bij de wet van 1 juni 2008, vervangen bij de wet van 21 december 2009 en gewijzigd bij de wet van 8 mei 2014, worden" / "À l'article 145³² du même Code, inséré par la loi du 1^{er} juin 2008, remplacé par la loi du 21 décembre 2009 et modifié par la loi du 8 mai 2014, les modifications"*.
- Art. 63, 3^o: *"in paragraaf 3 wordt de inleidende zin vervangen als volgt:" / "3^o dans le paragraphe 3, la phrase liminaire est remplacée par ce qui suit:".*
Dezelfde opmerking geldt mutatis mutandis voor de bepaling onder 4^o van hetzelfde artikel.
- Art. 64: *"In titel II, hoofdstuk III, afdeling 1, van hetzelfde Wetboek, wordt de onderafdeling IIterdecies "-Vermindering voor uitgaven voor een ontwikkelingsfonds – Terugname van de vermindering", die het artikel 145³² bevat, ingevoegd bij de wet van 1 juni 2008, vervangen bij de wet van 21 december 2009 en laatstelijk gewijzigd bij artikel 63, opgeheven." / "Dans le titre II, chapitre III, section 1^{re}, du même Code, la sous-section IIterdecies "- Réduction pour les dépenses consacrées à un fonds de développement – Reprise de la réduction", qui contient l'article 145³², insérée par la loi du 1^{er} juin 2008, remplacée par la loi du 21 décembre 2009 et modifiée en dernier lieu par l'article 63, est abrogée."*
- Art. 70: *"In artikel 171, 6^o, van hetzelfde Wetboek, laatstelijk gewijzigd bij artikel 4, worden in de inleidende zin de woorden" / "Dans l'article 171, 6^o, du même Code, modifié en dernier lieu par l'article 4, dans la phrase liminaire, les mots"*.
- Art. 74: *"Artikel 198quater van hetzelfde Wetboek, ingevoegd bij de wet van 25 december 2017, zelf gewijzigd bij de wet van 2 mei 2019, wordt opgeheven." / "L'article 198quater du même Code, inséré par la loi du 25 décembre 2017, elle-même modifiée par la loi du 2 mai 2019, est abrogé."*
- Art. 80: *"In artikel 294, tweede lid, van hetzelfde Wetboek, ingevoegd bij de wet van 8 mei 2014 en laatstelijk gewijzigd bij de wet van 31 juli 2023, worden" / "À l'article 294, alinéa 2, du même Code, inséré par la loi du 8 mai 2014 et modifié en dernier lieu par la loi du 31 juillet 2023, dans le"*.
- Art. 87/2: *"In artikel 315bis, vijfde lid, van hetzelfde Wetboek, ingevoegd bij de wet van 6 juli 1994 en laatstelijk gewijzigd bij de wet van 20 november 2022, wordt" / "Dans l'article 315bis, alinéa 5, du même Code, inséré par la loi du 6 juillet 1994 et modifié en dernier lieu par la loi du 20 novembre 2022, le"*.
- Art. 89: *"In artikel 354 van hetzelfde Wetboek, vervangen bij de wet van 20 november 2022 en gewijzigd bij de wet van 22 december 2023, worden" / "À l'article 354 du même Code, remplacé par la loi du 20 novembre 2022 et modifié par la loi du 22 décembre 2023, les modifications"*.

- Art. 90/1: "*In artikel 60 van het Wetboek van de belasting over de toegevoegde waarde, vervangen bij de wet van 17 december 2012 en laatstelijk gewijzigd bij de wet van 23 november 2023, worden*" / "*À l'article 60 du Code de la taxe sur la valeur ajoutée, remplacé par la loi du 17 décembre 2012 et modifié en dernier lieu par la loi du 23 novembre 2023, les*".
- Art. 91: "*In artikel 81bis, § 1, van hetzelfde Wetboek, ingevoegd bij de wet van 15 maart 1999, vervangen bij de wet van 22 december 2008 en laatstelijk gewijzigd bij de wet van 23 november 2023, worden*" / "*À l'article 81bis, § 1^{er}, du même Code, inséré par la loi du 15 mars 1999, remplacé par la loi du 22 décembre 2008 et modifié en dernier lieu par la loi du 23 novembre 2023, les modifications*".
- Art. 95/1: "*In Boek II, Titel X, van het Wetboek diverse rechten en taksen, wordt*" / "*Dans le Livre II, Titre X, du Code des droits et taxes divers, il*".

N.B.: Enkele minder belangrijke verbeteringen werden op een exemplaar van de tekst aan het commissiesecretariaat bezorgd.

NOTE À L'ATTENTION DE LA COMMISSION DES FINANCES ET DU BUDGET

Objet: Note de légistique relative aux articles adoptés en première lecture du projet de loi portant des dispositions diverses (*partim* Finances: art. 1^{er} à 95/8) (DOC 56-0963/020).

OBSERVATIONS GÉNÉRALES

1. Dans le titre 2, chapitre 1^{er}, section 11, sous-section 1^{re}, du projet de loi, plusieurs articles du Code des impôts sur les revenus 1992 (ci-après: "CIR 92") sont abrogés. Il appartient à la commission de vérifier et de modifier les renvois à ces articles abrogés, et ce, non seulement dans le CIR 92, mais également dans d'autres lois. À titre d'illustration, citons de manière non exhaustive les articles suivants, qui ne sont pas modifiés par le projet de loi, mais qui contiennent bel et bien un renvoi à l'un des articles abrogés du CIR 92:
 - l'article 145²⁶, § 3, alinéa 3, 1^o, du CIR 92, qui renvoie à l'article 145³² du CIR 92, lequel est abrogé par l'article 64 du projet de loi;
 - l'article 145²⁷, § 2, alinéa 5, 1^o, du CIR 92, qui renvoie à l'article 145³² du CIR 92 abrogé;
 - l'article 175 du CIR 92, qui renvoie à l'article 145³², § 2, du CIR 92 abrogé;
 - l'article 531 du CIR 92, qui renvoie à l'article 67, § 4, du CIR 92, lequel est abrogé par l'article 55 du projet de loi;
 - l'article 10, § 1^{er}, alinéa 2, de la loi du 17 mars 2019 'concernant l'instauration d'un budget mobilité', qui renvoie à l'article 145²⁸ du CIR 92, lequel est abrogé par l'article 62 du projet de loi.

Lors de la modification des renvois aux articles abrogés du CIR 92, la commission devra tenir compte des différentes dates auxquelles les dispositions abrogatoires entreront en vigueur, tel que prévu dans l'article 87 du projet de loi.

2. Les articles 85 et 86 du projet de loi abrogent respectivement les articles 2 et 3 de la loi du 1^{er} juin 2008 'instaurant une réduction d'impôt pour les participations sous la forme d'actions dans des fonds de développement du microfinancement dans les pays en développement et fixant les conditions d'agrément en tant que fonds de développement'. Il appartient à la commission de vérifier et de modifier les renvois à ces articles abrogés dans d'autres lois, en tenant compte du fait que les articles 85 et 86 du projet de loi n'entreront en vigueur que le 1^{er} janvier 2031 en vertu de l'article 87, alinéa 7, du projet de loi.

À titre d'illustration, citons de manière non exhaustive l'article 180, § 2, 2^o, de la loi du 19 avril 2014 'relative aux organismes de placement collectif alternatifs et à leurs gestionnaires', qui renvoie aux "*fonds de développement visés à l'article 2, 1^o de la loi du 1^{er} juin 2008 (...)*".

OBSERVATIONS PARTICULIÈRES RELATIVES AUX ARTICLES

Art. 41

3. On insérera dans l'article 41 du projet de loi un c)/1 rédigé comme suit:

"c)/1. dans le paragraphe 3, dans l'alinéa 4 ancien, devenant l'alinéa 5, les mots "conformément à l'alinéa 3, 2^o" sont remplacés par les mots "conformément à l'alinéa 4, 2^o";"

/

c)/1. in paragraaf 3, in het vroegere vierde lid, dat het vijfde lid wordt, worden de woorden "overeenkomstig het derde lid, 2^o" vervangen door de woorden "overeenkomstig het vierde lid, 2^o";".

(Modification du renvoi croisé dans l'une des subdivisions du paragraphe 3 de l'article 178 du CIR 92 à la suite de l'insertion dans ce paragraphe, par le c), d'un alinéa entre les alinéas 2 et 3.)

Art. 41/1

4. On insérera dans le projet de loi un nouvel article 41/1 rédigé comme suit:

"Art. 41/1. Dans l'article 70 de la loi du 5 juillet 2022 portant des dispositions fiscales diverses, les mots "Dans l'article 178, § 3, alinéa 3, du même Code" sont remplacés par les mots "Dans l'article 178, § 3, alinéa 4, du même Code"."

/

"Art. 41/1. In artikel 70 van de wet van 5 juli 2022 houdende diverse fiscale bepalingen worden de woorden "In artikel 178, § 3, derde lid, van hetzelfde Wetboek" vervangen door de woorden "In artikel 178, § 3, vierde lid, van hetzelfde Wetboek"."

(L'article 70 de la loi du 5 juillet 2022 'portant des dispositions fiscales diverses', qui, en vertu de l'article 71, alinéa 17, de la même loi, sera applicable à partir de l'exercice d'imposition 2028, modifie la phrase liminaire de l'article 178, § 3, alinéa 3, du CIR 92. Toutefois, à la suite de la modification apportée par l'article 41, c), du projet de loi, qui, en vertu de l'article 42 du projet de loi, sera déjà applicable à partir de l'exercice d'imposition 2026, l'alinéa 3 de l'article 178, § 3, du CIR 92 deviendra l'alinéa 4. Le nouvel article 41/1 proposé vise à adapter la partie de l'article 178, § 3, du CIR 92 dans laquelle la modification prévue par l'article 70 de la loi du 5 juillet 2022 doit être apportée à la modification prévue par l'article 41, c), du projet de loi.)

Si la commission suit cette observation, on remplacera, dans la phrase liminaire de l'article 43 du projet de loi, les mots *"du même Code" / "van hetzelfde Wetboek"* par les mots *"du Code des impôts sur les revenus 1992" / "van het Wetboek van de inkomstenbelastingen 1992"*.

Art. 60

5. L'article 51 du projet de loi abroge l'article 38, § 1^{er}, alinéa 1^{er}, 17^o, du CIR 92 et, en vertu de l'article 87, alinéa 1^{er}, du projet de loi, cette abrogation produira ses effets à partir du 30 septembre 2025. L'article 60, 1^o, du projet de loi abroge, dans l'article 129/1, alinéa 1^{er}, du CIR 92, le renvoi à l'article 38, § 1^{er}, alinéa 1^{er}, 17^o, du CIR 92, cette abrogation s'appliquant à partir de l'exercice d'imposition 2027 en vertu de l'article 87, alinéa 5, du projet de loi. Cela signifie que, jusqu'à l'exercice d'imposition 2027, l'article 129/1, alinéa 1^{er}, du CIR 92 renverra au montant mentionné à l'article 38, § 1^{er}, alinéa 1^{er}, 17^o, du CIR 92 alors

que cette disposition aura déjà été abrogée avec effet au 30 septembre 2025. Il convient donc de se demander si, dans l'article 129/1, alinéa 1^{er}, du CIR 92, le renvoi à l'article 38, § 1^{er}, alinéa 1^{er}, 17°, du CIR 92 ne doit pas d'abord être remplacé par un renvoi à *"l'article 38, § 1^{er}, alinéa 1^{er}, 17°, tel qu'il existait avant son abrogation par l'article 51 de la loi du ... portant des dispositions diverses"* avant d'abroger définitivement le renvoi à partir de l'exercice d'imposition 2027.

Art. 76

6. Dans le a), qui modifie la phrase liminaire de l'article 243/1 du CIR 92, les mots "145²⁶, 145²⁸, 145³² à 145³⁵, 145⁴⁸," sont remplacés par les mots "145²⁶, 145³³, 145³⁵". Cette disposition modificative présente deux manquements:
7. la phrase liminaire de l'article 243/1 du CIR 92 renvoie en réalité aux mots "145²⁶ à 145²⁸", au lieu des mots "145²⁶, 145²⁸", de sorte que la phrase liminaire renvoie désormais également à l'article 145^{26/1} du CIR 92, qui sera abrogé par l'article 61 du projet de loi, et à l'article 145²⁷ du CIR 92, qui ne sera pas abrogé par le projet de loi;
8. la phrase liminaire de l'article 243/1 du CIR 92 renvoie désormais également à l'article 145⁵⁰ du CIR 92², qui sera abrogé par l'article 69 du projet de loi.

La question se pose dès lors de savoir si, dans la phrase liminaire de l'article 243/1 du CIR 92, les mots "145²⁶ à 145²⁸, 145³² à 145³⁵, 145⁴⁸, 145⁵⁰" ne devraient pas être remplacés par les mots "145²⁶, 145²⁷, 145³³, 145³⁵". Cela permettrait, d'une part, de mettre fin au renvoi aux articles 145^{26/1} et 145⁵⁰ abrogés du CIR 92 et, d'autre part, de maintenir le renvoi à l'article 145²⁷ du CIR 92, qui ne sera pas abrogé par le projet de loi. La modification proposée n'est d'ailleurs pas en contradiction avec l'entrée en vigueur des dispositions concernées fixée par l'article 87 du projet de loi, dès lors qu'en vertu de l'article 87, alinéa 4, du projet de loi, tant l'abrogation des articles 145^{26/1} et 145⁵⁰ du CIR 92 que l'article 76, a), du projet de loi s'appliqueront à partir de l'exercice d'imposition 2026.

Il appartient à la commission de réexaminer l'article 76, a), du projet de loi.

9. Dans le c), qui modifie l'article 243/1, 4°, du CIR 92, les mots "145^{26/1}, §§ 1^{er} et 2, 145²⁷, §§ 1^{er} à 3, 145²⁸, 145³², § 1^{er}, 145³³ à 145³⁵, 145⁴⁸," sont remplacés par les mots "145²⁷, §§ 1^{er} à 3, 145³³, 145³⁵". Étant donné que l'article 243/1, 4°, du CIR 92 renvoie désormais également à l'article 145⁵⁰ du CIR 92³, qui sera abrogé par l'article 69 du projet de loi, la question se pose de savoir si, dans l'article 243/1, 4°, du CIR 92, les mots "145^{26/1}, §§ 1^{er} et 2, 145²⁷, §§ 1^{er} à 3, 145²⁸, 145³², § 1^{er}, 145³³ à 145³⁵, 145⁴⁸, 145⁵⁰" ne devraient pas plutôt être remplacés par les mots "145²⁷, §§ 1^{er} à 3, 145³³, 145³⁵". La modification proposée n'est d'ailleurs pas en contradiction avec l'entrée en vigueur des dispositions concernées fixée par l'article 87 du projet de loi, dès lors qu'en vertu de l'article 87, alinéa 4, du projet de loi, tant l'abrogation de l'article 145⁵⁰ du CIR 92 que l'article 76, c), du projet de loi s'appliqueront à partir de l'exercice d'imposition 2026.

¹ L'article 35, 1°, de la loi du 26 mars 2018 'relative au renforcement de la croissance économique et de la cohésion sociale' a remplacé les mots "145²⁶, 145²⁸" par les mots "145²⁶ à 145²⁸" dans la phrase liminaire de l'article 243/1 du CIR 92.

² L'article 19, 1°, de la loi du 25 novembre 2021 'organisant le verdissement fiscal et social de la mobilité' a remplacé les mots "145⁴⁸, 146 à 154bis" par les mots "145⁴⁸, 145⁵⁰, 146 à 154bis" dans la phrase liminaire de l'article 243/1 du CIR 92.

³ L'article 19, 2°, de la loi du 25 novembre 2021 'organisant le verdissement fiscal et social de la mobilité' a remplacé les mots "145⁴⁸, 154bis" par les mots "145⁴⁸, 145⁵⁰, 154bis" dans l'article 243/1, 4°, du CIR 92.

Art. 87

10. L'article 87 du projet de loi fixe l'entrée en vigueur de tous les articles relevant du titre 2, chapitre 1^{er}, section 11, sous-sections 1^{re} et 2, du projet de loi, à savoir les articles 51 à 86. Pour un article, à savoir l'article 70 du projet de loi, l'entrée en vigueur n'est toutefois pas réglée. Ce dernier article abroge, dans la phrase liminaire du 6^o de l'article 171 du CIR 92, le renvoi aux articles 145^{26/1}, 145²⁸, 145³², 145³⁴, 145⁴⁸, 145⁴⁹ et 145⁵⁰ abrogés du même Code.

Dès lors que les articles 61, 62 et 66 à 69 du projet de loi, qui abrogent respectivement les articles 145^{26/1}, 145²⁸, 145³⁴, 145⁴⁸, 145⁴⁹ et 145⁵⁰ du CIR 92, seront tous applicables à partir de l'exercice d'imposition 2026 et que la réduction d'impôt visée à l'article 145³² du CIR 92 ne sera plus accordée à partir de l'exercice d'imposition 2026⁴, la question se pose de savoir si l'article 87, alinéa 4, du projet de loi ne doit pas être complété par un renvoi à l'article 70 du projet de loi.

Art. 92

11. Alors que l'actuel article 84^{ter} du Code de la taxe sur la valeur ajoutée (ci-après: "Code de la TVA") vise "*les indices de fraude*" / "*aanwijzingen van fraude*", l'article 84^{ter} en projet du Code de la TVA vise, en français, "*les indices de fraude fiscale*" et, en néerlandais, "*aanwijzingen van fraude*". Il convient de se demander quelle version linguistique est correcte et, plus fondamentalement, quelle fraude est visée.⁵

La même observation s'applique à l'article 93 du projet de loi (future version de l'article 84^{ter} du Code de la TVA.)

Art. 93

12. L'article 84^{ter} du Code de la TVA sera remplacé par l'article 92 du projet de loi, qui entrera en vigueur le dixième jour suivant la publication de la loi à adopter au *Moniteur belge*. L'article 84^{ter} du Code de la TVA sera toutefois également remplacé par l'article 56 de la loi du 12 mai 2024 'visant à digitaliser les relations entre le Service public fédéral Finances, les citoyens, les entreprises, les personnes morales et certains tiers et abrogeant la loi du 26 janvier 2021 sur la dématérialisation des relations entre le Service public fédéral Finances, les citoyens, personnes morales et certains tiers, et modifiant différents codes fiscaux et lois fiscales', qui entrera en vigueur à une date à fixer par le Roi et au plus tard le 1^{er} janvier 2028⁶. La modification prévue à l'article 92 du projet de loi risque ainsi d'être annulée au moment où l'article 56 de la loi du 12 mai 2024 entrera en vigueur. Pour y remédier, il a été décidé de remplacer à nouveau l'article 84^{ter} du Code de la TVA dans l'article 93 du projet de loi, en tenant compte à la fois de la modification visée à l'article 92 du projet de loi et de celle visée à l'article 56 de la loi du 12 mai 2024, de manière à faire coïncider l'entrée en vigueur de l'article 93 du projet de loi avec celle de l'article 56 de la loi du 12 mai 2024.⁷ La phrase liminaire de l'article 93 du projet de loi, dans sa formulation actuelle, n'élimine toutefois pas ce risque: étant donné que l'article 56 de la loi du 12 mai 2024 ne sera pas abrogé, il n'apparaît pas clairement si, à la date d'entrée en vigueur

⁴ Voir le commentaire des articles 63 et 64 du projet de loi: DOC 56-0963/001, p. 36-37.

⁵ Voir le commentaire de l'article 92 du projet de loi: DOC 56-0963/001, p. 41: "*Il est maintenant prévu que cette notification mentionne préalablement au redressement et de manière précise, à la personne concernée, les indices de fraude fiscale qui existent, à son encontre.*" (soulignement par nos soins).

⁶ Art. 222 de la loi du 12 mai 2024.

⁷ Voir le commentaire de l'article 93 du projet de loi: DOC 56-0963/001, p. 41.

fixée, le remplacement visé à l'article 93 du projet de loi ou celui visé à l'article 56 de la loi du 12 mai 2024 devra être appliqué en premier. Ce risque peut être évité:

- soit en modifiant l'article 56 de la loi du 12 mai 2024 pour tenir compte de la modification prévue par l'article 92 du projet de loi, au lieu d'intervenir à nouveau directement dans l'article 84^{ter} du Code de la TVA;
- soit en abrogeant l'article 56 de la loi du 12 mai 2024, cette abrogation devant entrer en vigueur au plus tard la veille de la date d'entrée en vigueur dudit article. Dans ce cas, on remplacera, dans la phrase liminaire de l'article 93 du projet de loi, les mots "*remplacé par la loi du 23 novembre 2023*" / "*vervangen bij de wet van 23 november 2023*" par les mots "*remplacé par l'article 92*" / "*vervangen bij artikel 92*";
- soit en indiquant clairement, dans la phrase liminaire de l'article 93 du projet de loi, qu'il a été tenu compte de la disposition modificative qui n'est pas encore entrée en vigueur.⁸

Si la commission opte pour cette dernière solution, on remplacera la phrase liminaire de l'article 93 du projet de loi par ce qui suit: "*L'article 84^{ter} du même Code, inséré par la loi du 15 mars 1999, remplacé par l'article 92 et tel que remplacé par la loi du 12 mai 2024, est remplacé par ce qui suit:*" / "*Artikel 84^{ter} van hetzelfde Wetboek, ingevoegd bij de wet van 15 maart 1999, vervangen bij artikel 92 en zoals vervangen bij de wet van 12 mei 2024, wordt vervangen als volgt:*".

AMÉLIORATIONS PUREMENT FORMELLES ET CORRECTIONS D'ORDRE PUREMENT LINGUISTIQUE

Art. 2

- 13.** Dans le texte français du 2°, on remplacera les mots "*et les mots 'les intérêts et' sont abrogés;*" par les mots "*et les mots 'les intérêts et redevances visés à l'alinéa 1^{er}, ne sont déductibles que lorsqu'ils ont été payés pendant' sont remplacés par les mots 'les redevances visées à l'alinéa 1^{er}, ne sont déductibles que lorsqu'elles ont été payées pendant';*".

(Correction d'ordre linguistique.)

Art. 14

- 14.** Dans l'alinéa 2, on remplacera les mots "*contrats d'assurance-vie conclus individuellement et des emprunts*" / "*levensverzekeringscontracten en leningsovereenkomsten*" par les mots "*contrats d'assurance-vie conclus individuellement et des emprunts hypothécaires*" / "*levensverzekeringscontracten en hypothecaire leningsovereenkomsten*".

(La terminologie de la disposition est alignée sur celle de l'article 323/1, § 1^{er}, alinéa 1^{er}, du CIR 92, tel que modifié par l'article 8, 1°, du projet de loi.)

Art. 23

- 15.** Dans le 8°, dans l'article 66, § 4, du CIR 92, en projet, on remplacera les mots "*Par dérogation aux paragraphes 1^{er} et 1^{er}/1 du présent article et à l'article 550*" / "*In afwijking van de paragrafen 1 en 1/1 van dit artikel en artikel 550*" par les mots "*Par dérogation aux paragraphes 1^{er} et 1^{er}/1 et à l'article 550*" / "*In afwijking van de paragrafen 1 en 1/1 en artikel 550*".

⁸ Conseil d'État, *Principes de technique législative. Guide de rédaction des textes législatifs et réglementaires*, 2008, p. 84, nos 130-131.

(Correction d'ordre légistique: lorsqu'une référence est établie à l'intérieur d'une même division d'un texte, il est inutile de rappeler qu'il s'agit de la même division.⁹)

Art. 41

16. Dans le texte néerlandais du c), dans l'article 178, § 3, alinéa 3, du CIR 92, en projet, on remplacera les mots "*indexcijfers van het jaar van de inkomsten voorafgaat*" par les mots "*indexcijfers van het jaar dat het jaar van de inkomsten voorafgaat*".

(Concordance avec le texte français: "... des indices des prix de l'année qui précède celle des revenus ...".)

Art. 43

17. Dans le texte français de l'article 206/3, § 1^{er}, alinéa 2, deuxième tiret, du CIR 92, en projet, on remplacera les mots "*avant la reprise du transfert intra-groupe repris dans la base*" par les mots "*avant la reprise du transfert intra-groupe dans la base*".

(Le mot "*repris*" a été supprimé en raison de son double emploi avec les mots "*la reprise*" et parce qu'il ne possède pas d'équivalent dans le texte néerlandais.)

Art. 89/1 (nouveau)

18. Dans le texte néerlandais de l'article 354/1 du CIR 92, en projet, on remplacera, dans la phrase liminaire, les mots "*De bijkomende termijn*" par les mots "*De aanvullende termijn*".

(Concordance des termes de la disposition en projet avec ceux de l'article 333, alinéa 3, du CIR 92, en projet [art. 88 du projet de loi], ainsi qu'avec ceux de la phrase liminaire de l'actuel article 354/1 du CIR 92.)

Art. 95/1 (nouveau)

19. Dans l'article 201/9/7, § 1^{er}, alinéa 1^{er}, du Code des droits et taxes divers, en projet, on remplacera les mots "*à l'article 4, 1^o/1 de la loi*" / "*in artikel 4, 1^o/1 van de voornoemde wet*" par les mots "*à l'article 4, alinéa 1^{er}, 1^o/1, de la loi*" / "*in artikel 4, eerste lid, 1^o/1, van de voornoemde wet*".

(Précision de la référence.)

Art. 95/2 (nouveau)

20. On remplacera les mots "*à la date visée à l'article 95/8 de la présente loi*" / "*de dag bepaald in artikel 95/8 van deze wet*" par les mots "*à la date visée à l'article 95/8, alinéa 1^{er}*" / "*de datum bepaald in artikel 95/8, eerste lid*".

(Précision de la référence et harmonisation des deux versions linguistiques. + Correction d'ordre légistique: lorsqu'on établit une référence à l'intérieur d'un même texte, on ne rappelle pas qu'il s'agit du même texte.¹⁰)

⁹ Conseil d'État, o.c., p. 59, n° 72, a).

¹⁰ Conseil d'État, o.c., p. 59, n° 72, a).

CORRECTIONS RELATIVES AUX PHRASES LIMINAIRES DES ARTICLES

- Art. 2: "À l'article 14 du Code des impôts sur les revenus 1992, ~~remplacé par la loi du 6 juillet 1994~~ et modifié en dernier lieu par la loi du 21 janvier 2022, les modifications" / "In artikel 14 van het Wetboek van de inkomstenbelastingen 1992, ~~vervangen bij de wet van 6 juli 1994~~ en laatstelijk gewijzigd bij de wet van 21 januari 2022, worden".
- Art. 4, b): "au 6°, ~~dans la phrase liminaire~~, le nombre" / "in de bepaling onder 6° wordt ~~in de inleidende zin~~ het nummer".
- Art. 21: "Dans l'article 36, § 2, alinéa 9, du même Code, ~~inséré par la loi du 25 décembre 2017, elle-même modifiée par la loi du 2 mai 2019, et modifié par la loi du 27 juin 2021, les mots~~" / "In artikel 36, § 2, negende lid, van hetzelfde Wetboek, ~~ingevoegd bij de wet van 25 december 2017, zelf gewijzigd bij de wet van 2 mei 2019, en gewijzigd bij de wet van 27 juni 2021, worden~~".
- Art. 22, 5°: "le paragraphe 1^{er}/1, alinéa 2, remplacé par le 3° ~~et modifié par le 4°~~, est complété" / "paragraaf 1/1, tweede lid, vervangen ~~bij de bepaling onder 3° en gewijzigd bij de bepaling onder 4°~~, wordt aangevuld".
- Art. 29: "Dans l'article 72 du même Code, ~~modifié par l'arrêté royal du 20 juillet 2000, lui-même modifié par l'arrêté royal du 13 juillet 2001, l'alinéa 2~~" / "In artikel 72 van hetzelfde Wetboek, ~~gewijzigd bij het koninklijk besluit van 20 juli 2000, zelf gewijzigd bij het koninklijk besluit van 13 juli 2001, wordt~~".
- Art. 38: "À l'article 145 du même Code, remplacé par la loi du 18 décembre 2016 ~~et modifié par la loi du 17 mars 2019, les~~" / "In artikel 145 van hetzelfde Wetboek, vervangen bij de wet van 18 december 2016 ~~en gewijzigd bij de wet van 17 maart 2019, worden~~".
- Art. 46: "L'article 246, alinéa 1^{er}, du même Code, ~~modifié en dernier lieu par la loi du 18 juillet 2025, est complété~~" / "Artikel 246, eerste lid, van hetzelfde Wetboek, ~~laatstelijk gewijzigd bij de wet van 18 juli 2025, wordt aangevuld~~".
- Art. 49: "Dans l'article 289bis, § 1^{er}, alinéa 1^{er}, phrase liminaire, du même Code, ~~inséré par la loi du 20 décembre 1995 et remplacé par la loi du 8 mai 2014, les~~" / "In artikel 289bis, § 1, eerste lid, inleidende zin, van hetzelfde Wetboek, ~~ingevoegd bij de wet van 20 december 1995 en~~ vervangen bij de wet van 8 mei 2014, worden".
- Art. 58: "Dans le titre II, chapitre II, section 4, sous-section 3, B, du même Code, la partie "1^{er}ter Personnel supplémentaire", qui comprend l'article 67ter, ~~insérée par la loi du 8 juin 2008 et modifiée par l'article 57, est abrogée~~" / "In titel II, hoofdstuk II, afdeling 4, onderafdeling 3, B, van hetzelfde Wetboek, wordt het onderdeel "1^{er}ter Bijkomend personeel", dat het artikel 67ter bevat, ingevoegd bij de wet van 8 juni 2008 ~~en gewijzigd bij artikel 57, opgeheven~~".
- Art. 63: "À l'article 145³² du même Code, ~~inséré par la loi du 1^{er} juin 2008, remplacé par la loi du 21 décembre 2009 et modifié par la loi du 8 mai 2014, les modifications~~" / "In artikel 145³² van hetzelfde Wetboek, ingevoegd bij de wet van 1 juni 2008, ~~vervangen bij de wet van 21 december 2009 en gewijzigd bij de wet van 8 mei 2014, worden~~".

- Art. 63, 3°: "3° dans le paragraphe 3, la phrase liminaire est remplacée par ce qui suit:" / "in paragraaf 3 wordt de inleidende zin vervangen als volgt:".
La même observation s'applique mutatis mutandis au 4° du même article.
- Art. 64: "Dans le titre II, chapitre III, section 1^{re}, du même Code, la sous-section IIterdecies "Réduction pour les dépenses consacrées à un fonds de développement – Reprise de la réduction", qui contient l'article 145³², insérée par la loi du 1^{er} juin 2008, remplacée par la loi du 21 décembre 2009 et modifiée en dernier lieu par l'article 63, est abrogée." / "In titel II, hoofdstuk III, afdeling 1, van hetzelfde Wetboek, wordt de onderafdeling IIterdecies "Vermindering voor uitgaven voor een ontwikkelingsfonds – Terugname van de vermindering", die het artikel 145³² bevat, ingevoegd bij de wet van 1 juni 2008, vervangen bij de wet van 21 december 2009 en laatstelijk gewijzigd bij artikel 63, opgeheven.".
- Art. 70: "Dans l'article 171, 6°, du même Code, modifié en dernier lieu par l'article 4, dans la phrase liminaire, les mots" / "In artikel 171, 6°, van hetzelfde Wetboek, laatstelijk gewijzigd bij artikel 4, worden in de inleidende zin de woorden".
- Art. 74: "L'article 198quater du même Code, inséré par la loi du 25 décembre 2017, elle-même modifiée par la loi du 2 mai 2019, est abrogé." / "Artikel 198quater van hetzelfde Wetboek, ingevoegd bij de wet van 25 december 2017, zelf gewijzigd bij de wet van 2 mei 2019, wordt opgeheven.".
- Art. 80: "À l'article 294, alinéa 2, du même Code, inséré par la loi du 8 mai 2014 et modifié en dernier lieu par la loi du 31 juillet 2023, dans le" / "In artikel 294, tweede lid, van hetzelfde Wetboek, ingevoegd bij de wet van 8 mei 2014 en laatstelijk gewijzigd bij de wet van 31 juli 2023, worden".
- Art. 87/2: "Dans l'article 315bis, alinéa 5, du même Code, inséré par la loi du 6 juillet 1994 et modifié en dernier lieu par la loi du 20 novembre 2022, le" / "In artikel 315bis, vijfde lid, van hetzelfde Wetboek, ingevoegd bij de wet van 6 juli 1994 en laatstelijk gewijzigd bij de wet van 20 november 2022, wordt".
- Art. 89: "À l'article 354 du même Code, remplacé par la loi du 20 novembre 2022 et modifié par la loi du 22 décembre 2023, les modifications" / "In artikel 354 van hetzelfde Wetboek, vervangen bij de wet van 20 november 2022 en gewijzigd bij de wet van 22 december 2023, worden".
- Art. 90/1: "À l'article 60 du Code de la taxe sur la valeur ajoutée, remplacé par la loi du 17 décembre 2012 et modifié en dernier lieu par la loi du 23 novembre 2023, les" / "In artikel 60 van het Wetboek van de belasting over de toegevoegde waarde, vervangen bij de wet van 17 december 2012 en laatstelijk gewijzigd bij de wet van 23 november 2023, worden".
- Art. 91: "À l'article 81bis, § 1^{er}, du même Code, inséré par la loi du 15 mars 1999, remplacé par la loi du 22 décembre 2008 et modifié en dernier lieu par la loi du 23 novembre 2023, les modifications" / "In artikel 81bis, § 1, van hetzelfde Wetboek, ingevoegd bij de wet van 15 maart 1999, vervangen bij de wet van 22 december 2008 en laatstelijk gewijzigd bij de wet van 23 november 2023, worden".



Juridische Zaken
Affaires juridiques

- Art. 95/1: "Dans le Livre II, Titre X, du Code des droits et taxes divers, il" / "In Boek II, Titel X, van het Wetboek diverse rechten en taksen, wordt".

N.B.: Quelques corrections moins importantes ont été communiquées sur un exemplaire du texte au secrétariat de la commission.