

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

27 februari 2026

BELEIDSNOTA

van de minister van Modernisering
van de overheid, belast met
Overheidsbedrijven, Ambtenarenzaken,
het Gebouwenbeheer van de Staat,
Digitalisering en Wetenschapsbeleid
(*partim*: Privacy)

Gedachtewisseling

Verslag
namens de commissie
voor Justitie
uitgebracht door
de heer **Christoph D’Haese**

Inhoud Blz.

I. Inleidende uiteenzetting	3
II. Bespreking.....	3
A. Vragen en opmerkingen van de leden.....	3
B. Antwoorden van de minister	23
C. Replieken van de leden	33
D. Bijkomende antwoorden van de minister	34

Zie:

Doc 56 1280/ (2025/2026):
001: Wetsontwerp.
002 en 003: Amendementen.

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

27 février 2026

NOTE DE POLITIQUE GÉNÉRALE

de la ministre de l’Action et
de la Modernisation publiques, chargée
des Entreprises publiques, de la Fonction
publique, de la Gestion immobilière de l’État,
du Numérique et de la Politique scientifique
(*partim*: Vie privée)

Échange de vues

Rapport
fait au nom de la commission
de la Justice
par
M. **Christoph D’Haese**

Sommaire Pages

I. Exposé introductif.....	3
II. Discussion	3
A. Questions et observations des membres.....	3
B. Réponses de la ministre	23
C. Répliques des membres	33
D. Réponses complémentaires de la ministre	34

Voir:

Doc 56 1280/ (2025/2026):
001: Projet de loi.
002 et 003: Amendements.

**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: Ismaël Nuino

A. — Vaste leden / Titulaires:

N-VA	Christoph D'Haese, Sophie De Wit, Kristien Van Vaerenbergh
VB	Marijke Dillen, Alexander Van Hoecke
MR	Philippe Goffin, Pierre Jadoul
PS	Khalil Aouasti, Lydia Mutyebele Ngoi
PVDA-PTB	Greet Daems, Julien Ribaud
Les Engagés	Ismaël Nuino, Aurore Tourneur
Vooruit	Alain Yzermans
cd&v	Steven Matheï
Ecolo-Groen	Stefaan Van Hecke
Anders.	Katja Gabriëls

B. — Plaatsvervangers / Suppléants:

Jeroen Bergers, Maaïke De Vreese, Wim Van der Donckt, Charlotte Verkeyn
Katleen Bury, Werner Somers, Francesca Van Belleghem
Catherine Delcourt, Anthony Dufrane, Victoria Vandenberg
Caroline Désir, Pierre-Yves Dermagne, Patrick Prévot
Kemal Bilmez, Nabil Boukili, Kim De Witte
Serge Hilgsmann, Pierre Kompany, Marc Lejeune
Brent Meuleman, Axel Weydts
Leentje Grillaert, Els Van Hoof
Sarah Schlitz, Matti Vandemaele
Alexia Bertrand, Paul Van Tigchelt

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
Anders.	: Anders.
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)

DAMES EN HEREN,

Uw commissie heeft de beleidsnota van de minister van Modernisering van de overheid, belast met Overheidsbedrijven, Ambtenarenzaken, het Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid (*partim*: Privacy) besproken tijdens haar vergadering van 4 februari 2026.

I. — INLEIDENDE UITEENZETTING

Mevrouw Vanessa Matz, minister van Modernisering van de overheid, belast met Overheidsbedrijven, Ambtenarenzaken, het Gebouwenbeheer van de Staat, Digitalisering en Wetenschapsbeleid, zet de krachtlijnen uiteen van haar beleidsnota (DOC 56 1282/032).

II. — BESPREKING

A. Vragen en opmerkingen van de leden

De heer Christoph D'Haese (N-VA) stelt vooreerst vast dat er op het beleidsdomein van de minister het afgelopen jaar nog niet ontzettend veel is veranderd. Tegelijk kan men haar hiervoor verschonen.

Het eerste jaar van deze regering is immers snel voorbijgegaan: kabinetten moesten worden samengesteld, er was een kennismaking met de verschillende administraties en er vonden intensieve begrotingsbesprekingen plaats. De details van heel wat hervormingen uit het regeerakkoord moesten verder worden uitgewerkt, en het wetgevend werk voor een aantal van die hervormingen werd reeds opgestart.

De spreker sluit zich uiteraard aan bij de visie van de minister inzake de versterking van de Gegevensbeschermingsautoriteit (GBA), de manier waarop men met innovatie moet omgaan en ook de particulariteit rond het Controleorgaan op de Politie Informatie (COC).

In deze bespreking wil hij echter vooral ingaan op het feit dat binnen de commissie voor Justitie een belangrijke discussie aan de gang is met een aantal experts, onder meer over het voorstel van resolutie betreffende de opheffing van online anonimiteit en de instelling van een doeltreffende leeftijdscntrole voor toegang tot sociale media (DOC 56 1039/001). Die resolutie heeft een dubbele finaliteit: enerzijds de opheffing van online anonimiteit, anderzijds de invoering van een doeltreffende leeftijdscntrole voor toegang tot sociale media.

MESDAMES, MESSIEURS,

Votre commission a examiné la note de politique générale de la ministre de l'Action et de la Modernisation publiques, chargée des Entreprises publiques, de la Fonction publique, de la Gestion immobilière de l'État, du Numérique et de la Politique scientifique (*partim*: Vie privée), au cours de sa réunion du 4 février 2026.

I. — EXPOSÉ INTRODUCTIF

Mme Vanessa Matz, ministre de l'Action et de la Modernisation publiques, chargée des Entreprises publiques, de la Fonction publique, de la Gestion immobilière de l'État, du Numérique et de la Politique scientifique, expose les grandes lignes de sa note de politique générale (DOC 56 1282/032).

II. — DISCUSSION

A. Questions et observations des membres

M. Christoph D'Haese (N-VA) constate d'abord que, dans le domaine de compétence de la ministre, peu de changements majeurs sont intervenus au cours de l'année écoulée. On ne saurait toutefois lui en faire grief.

La première année de ce gouvernement est en effet passée rapidement: les cabinets ont dû être constitués, une prise de contact avec les différentes administrations a eu lieu et des discussions budgétaires intensives se sont tenues. Les détails de nombreuses réformes prévues par l'accord de gouvernement ont dû être précisés et le travail législatif relatif à certaines d'entre elles a déjà été entamé.

L'intervenant souscrit naturellement à la vision de la ministre en ce qui concerne le renforcement de l'Autorité de protection des données (APD), la manière d'appréhender l'innovation ainsi que la spécificité liée à l'Organe de contrôle des informations policières (COC).

Dans le cadre de cette discussion, il souhaite toutefois surtout aborder le fait qu'au sein de la commission de la Justice, un débat important est en cours avec plusieurs experts, notamment à propos de la proposition de résolution visant à mettre fin à l'anonymat en ligne et à instaurer un contrôle effectif de l'âge pour l'accès aux réseaux sociaux (DOC 56 1039/001). Cette résolution poursuit un double objectif: d'une part, la levée de l'anonymat en ligne et, d'autre part, l'introduction d'un contrôle de l'âge efficace pour l'accès aux réseaux sociaux.

Het zou interessant zijn dat de minister daarop een antwoord formuleert.

Het eerste punt waar men bij moetilstaan, is wat de minister de komende maanden wil doen. Dat doel kan legitiem zijn, maar de vraag is of ze ook de juiste aanpak heeft. Uit de hoorzitting van 3 februari 2026 over de problematiek is immers gebleken dat anonimiteit vaak gelijk wordt gesteld aan straffeloosheid, terwijl dat niet altijd terecht is. Bestaande instrumenten – zoals inlogverplichtingen voor platformen, IP-retentie onder Europese wetgeving en gerechtelijke identificatie bij concrete verdenking – maken vervolging van online misdrijven reeds mogelijk binnen de grenzen van de rechtsstaat.

De minister spreekt vaak over overleg. Wat zijn de te verwachten resultaten van het overleg met de minister van Justitie? En hoe verhoudt dat overleg zich tot het aangekondigde wetgevend initiatief dat zij hier zal indienen? Is dat initiatief voldoende?

Een tweede punt betreft de technische haalbaarheid. Een nationaal systeem voor geverifieerde pseudoanonymiteit en leeftijdsverificatie vereist een combinatie van ID-verificatie, vertrouwensregisters, platformkoppelingen, loginmechanismen en juridische toegangspoorten. Geloof de minister dat dit haalbaar is? Het lid zou graag een duidelijk antwoord krijgen. Op de hoorzitting hieromtrent bleek verdeeldheid. Het is dan ook relevant te vernemen hoe de minister met die inzichten zal omgaan en hoe zij deze commissie verder zal betrekken.

De minister heeft bovendien benadrukt dat fundamentele rechten voor haar zeer belangrijk zijn, waaronder het proportionaliteitsbeginsel. De AVG verplicht overheden om enkel persoonsgegevens te verwerken als dat noodzakelijk en proportioneel is voor een wettelijk doel. Een universele identiteitskoppeling, waarbij gevoelige data bij meerdere verwerkers wordt opgeslagen – en het lijkt erop dat de minister mogelijk in die richting wil gaan, al kan zij dat nuanceren – creëert een vorm van massale preventieve registratie. De vraag is of dat te rechtvaardigen valt. Dat is een essentieel punt in het kader van proportionaliteit en de eerbiediging van fundamentele rechten.

Tot slot wijst de spreker op het probleem van nationale fragmentatie en ineffectiviteit, waarover de minister wat op de vlakte blijft. Platformen zoals Meta, Google, X of

Il serait intéressant que la ministre formule une réponse à cet égard.

Le premier point à examiner concerne ce que la ministre entend faire dans les mois à venir. L'objectif peut être légitime, mais la question est de savoir si l'approche retenue est adéquate. Il ressort en effet de l'audition du 3 février 2026 consacrée à cette problématique que l'anonymat est souvent assimilé à l'impunité, ce qui n'est pas toujours justifié. Les instruments existants – tels que les obligations de connexion imposées aux plateformes, la conservation des adresses IP en vertu de la législation européenne et l'identification judiciaire en cas de suspicion concrète – permettent déjà de poursuivre les infractions en ligne dans les limites de l'État de droit.

La ministre évoque fréquemment la concertation. Quels sont les résultats attendus de la concertation avec le ministre de la Justice? Et comment cette concertation s'articule-t-elle avec l'initiative législative annoncée qu'elle entend déposer à la Chambre? Cette initiative est-elle suffisante?

Un deuxième point concerne la faisabilité technique. Un système national de pseudo-anonymat vérifié et de vérification de l'âge requiert une combinaison de vérification d'identité, de registres de confiance, d'interconnexions avec les plateformes, de mécanismes de connexion et de voies d'accès juridiques. La ministre estime-t-elle qu'un tel système est réalisable? Le membre souhaiterait obtenir une réponse claire à ce sujet. L'audition consacrée à cette question a en effet révélé des divergences d'appréciation. Il paraît dès lors pertinent de savoir comment la ministre entend tenir compte de ces éléments et de quelle manière elle associera davantage la commission aux travaux futurs.

La ministre a en outre souligné que les droits fondamentaux revêtaient pour elle une importance primordiale, notamment le principe de proportionnalité. Le RGPD impose aux autorités de ne traiter des données à caractère personnel que lorsque c'est nécessaire et proportionné à une finalité légale. Un lien universel avec l'identité, impliquant le stockage de données sensibles auprès de plusieurs responsables du traitement – et il semble que la ministre envisage peut-être une telle orientation, même si elle peut en nuancer la portée – créerait une forme d'enregistrement préventif massif. La question est de savoir si une telle mesure peut se justifier. Il s'agit d'un point essentiel au regard du principe de proportionnalité et du respect des droits fondamentaux.

Enfin, l'intervenant attire l'attention sur le problème de la fragmentation nationale et de l'inefficacité potentielle, sur lequel la ministre demeure relativement prudente.

Reddit hanteren uniforme authenticatie- en toegangsmodellen op mondiale schaal.

Wanneer één land afwijkende regels oplegt – zoals verplichte identiteitscontrole, lokale dataopslag of specifieke verificatie – is de meest waarschijnlijke reactie dat de platformen zullen overgaan tot “geoblocking”. Men probeert de wetgeving dan te neutraliseren door de dienst ontoegankelijk te maken voor gebruikers binnen een specifieke jurisdictie. Hoe gaat de minister daarmee om? Hoe verhoudt nationale wetgeving zich tot bestaande of hangende Europese initiatieven? En welke rol wil België daarin spelen? Ambieert de minister een voortrekkersrol?

Voor het overige onderschrijft de spreker volledig de doelstellingen zoals gesteld in de beleidsnota van de minister.

De heer Dieter Keuten (VB) benadrukt dat privacy en gegevensbescherming geen technische randkwesties meer zijn, maar aan de kern van de rechtsstaat raken: het briefgeheim, de bescherming van burgers tegen machtsmisbruik en de vraag wie controle heeft over data in een digitale samenleving.

De beleidsnota verwijst naar de evaluatie van het Controleorgaan op de Politie Informatie en naar een mogelijke verduidelijking van de privacywetgeving. Volgens de beschikbare informatie zijn er reeds stappen gezet, waaronder overleg met politiediensten en een brief aan de Kamer. De spreker vraagt of kan worden bevestigd dat deze evaluatie en de nieuwe privacywet nog dit jaar aan het Parlement zullen worden voorgelegd.

Vervolgens gaat hij in op de Gegevensbeschermingsautoriteit. Het jaarverslag toont een stijging van klachten met 21 % en 1455 datalekmeldingen, waarvan bijna de helft door menselijke fouten. Volgens hem is dit geen detail, maar een indicatie van structureel falen in digitale veiligheid.

Welke maatregelen neemt de regering tegen menselijke fouten als grootste oorzaak van datalekken? Wordt een federale verplichting tot minimale cybersecuritystandaarden voor overheden en vitale sectoren overwogen? Volstaan de hervorming en de uitbreiding van het personeelsbestand van de GBA, of blijft het

Des plateformes telles que Meta, Google, X ou Reddit appliquent des modèles d'authentification et d'accès uniformes à l'échelle mondiale.

Lorsqu'un pays impose des règles divergentes – telles qu'un contrôle d'identité obligatoire, un stockage local des données ou des mécanismes de vérification spécifiques – la réaction la plus probable des plateformes est le recours au géoblocage. Elles cherchent alors à neutraliser la législation en rendant le service inaccessible aux utilisateurs relevant d'une juridiction donnée. Comment la ministre entend-elle faire face à cette éventualité? Comment la législation nationale s'articule-t-elle avec les initiatives européennes existantes ou en cours? Et quel rôle la Belgique souhaite-t-elle jouer dans ce contexte? La ministre ambitionne-t-elle d'assumer un rôle moteur?

Pour le surplus, l'intervenant souscrit pleinement aux objectifs énoncés dans la note de politique générale de la ministre.

M. Dieter Keuten (VB) souligne que la protection de la vie privée et des données n'est plus une question marginale d'ordre technique, mais qu'elle touche au cœur même de l'État de droit. Elle concerne en effet le secret des lettres, la protection des citoyens contre les abus de pouvoir et la question du contrôle des données dans une société numérique.

La note de politique générale fait référence à l'évaluation de l'Organe de contrôle de l'information policière et à une éventuelle clarification de la législation sur la protection de la vie privée. Selon les informations disponibles, des mesures ont déjà été prises, dont une concertation avec les services de police et la rédaction d'une lettre adressée à la Chambre. L'intervenant demande s'il est possible de confirmer que cette évaluation et la nouvelle loi sur la protection de la vie privée seront soumises au Parlement avant la fin de l'année.

Il évoque ensuite la question de l'Autorité de protection des données. Le rapport annuel fait état d'une augmentation de 21 % des plaintes et de 1455 notifications de fuites de données, dont près de la moitié sont causées par des erreurs humaines. Selon lui, il ne s'agit pas d'un détail. Cette information indique une défaillance structurelle dans la sécurité numérique.

Quelles mesures le gouvernement prendra-t-il contre les erreurs humaines, principale cause des fuites de données? Une obligation fédérale de normes minimales en matière de cybersécurité pour les pouvoirs publics et les secteurs vitaux sera-t-elle envisagée? La réforme et l'augmentation de l'effectif de l'APD seront-elles

orgaan structureel onderbemand? Waarom is het aantal adviesaanvragen van overheden met 52 % gedaald?

Het Europese CSAM-voorstel, beter bekend als Chat Control, blijft een van de meest verontrustende dossiers. De beleidsnota stelt dat België actief zal deelnemen aan de onderhandelingen, met aandacht voor leeftijdscontrolemechanismen. Chat Control betekent in de praktijk dat elk privébericht van elke burger standaard wordt gescand. Dat vormt een breuk met het briefgeheim en een gevaarlijk precedent voor massasurveillance. Vandaag kan enkel een rechter gerichte interceptie toestaan – niet een algoritme, niet een ambtenaar. Automatische screening van iedereen gaat zeker niet op.

Wat is het standpunt van de regering over een Europees systeem dat neerkomt op algemene scanning van privécommunicatie?

Is de regering bereid het digitale briefgeheim expliciet te verankeren via een uitbreiding van artikel 29 van de Grondwet tot elektronische communicatie?

De spreker verwijst ook naar het voorstel betreffende de opheffing van online anonimiteit en de invoering van doeltreffende leeftijdscontrole. Deze werkzaamheden zijn erop gericht een Belgische wetgeving uit te werken met eerbiediging van het privacyrecht. Hoe wordt de toekomst van online anonimiteit gezien?

De beleidsnota verwijst naar artificiële intelligentie (AI) als modern opsporingsmiddel voor politie- en inlichtingendiensten. De spreker ondersteunt het vergemakkelijken van wetenschappelijk onderzoek op basis van gerechtelijke dossiers, zowel lopende als afgesloten, mits gegevensbescherming na te leven. Dit past in een bredere trend van datatoegang en evidencebased beleid, en biedt kansen om taboeonderwerpen objectiever te onderzoeken.

Tegelijk waarschuwt hij, verwijzend naar Hannah Arendt, voor systemen waarin menselijke beoordeling wordt vervangen door bureaucratische automatisering.

Welke garanties bestaan dat AI in opsporing nooit leidt tot automatische beslissingen zonder menselijke toets?

suffisantes ou l'organisme restera-t-il structurellement en sous-effectif? Pourquoi le nombre de demandes d'avis émanant des pouvoirs publics a-t-il diminué de 52 %?

La proposition de règlement CSAM (*Child Sexual Abuse Material*) de la Commission européenne, mieux connue sous le nom de *Chat Control*, reste l'un des dossiers les plus préoccupants. La note de politique générale précise que la Belgique participera activement aux négociations, en accordant une attention particulière aux mécanismes de contrôle de l'âge. En pratique, *Chat Control* signifie que chaque message privé de chaque citoyen sera scanné de façon standardisée. Cette façon de procéder marque une rupture avec le secret des lettres et constitue un dangereux précédent pour la surveillance de masse. Aujourd'hui, seul un juge peut autoriser une interception ciblée, et non un algorithme ou un fonctionnaire. Soumettre chaque citoyen à un analyse automatique n'est certainement pas acceptable.

Quelle est la position du gouvernement face à un système européen qui implique une analyse généralisée des communications privées?

Le gouvernement est-il disposé à ancrer explicitement le secret de la correspondance numérique en étendant l'article 29 de la Constitution aux communications électroniques?

L'intervenant fait également référence à la proposition de supprimer l'anonymat en ligne et d'introduire un contrôle efficace de l'âge. Ces travaux visent à se doter d'une législation belge respectueuse du droit à la vie privée. Comment envisage-t-on l'avenir de l'anonymat en ligne?

La note de politique générale fait référence à l'intelligence artificielle (IA) comme moyen d'investigation moderne pour les services de police et de renseignement. L'intervenant soutient l'idée de faciliter la recherche scientifique dans le cadre de dossiers judiciaires, aussi bien des dossiers en cours que clôturés, à condition de respecter la protection des données. Cette idée s'inscrit dans une tendance plus large d'accès aux données et de politique "*evidence-based*", et offre des opportunités pour étudier des sujets tabous de façon plus objective.

Parallèlement, il met en garde, en faisant référence à Hannah Arendt, contre les systèmes dans lesquels le jugement humain est remplacé par l'automatisation bureaucratique.

Quelles garanties existe-t-il qu'en matière d'enquêtes, l'IA ne conduira jamais à des décisions automatiques sans contrôle humain?

Komt er een parlementair controlemechanisme op het gebruik van AI door veiligheidsdiensten?

Daarnaast vraagt het lid hoe België zal garanderen dat AI-systemen die door overheid, politie of administraties worden ingezet niet onbewust persoonsgegevens memoreren en zo GDPR-schendingen veroorzaken. Hij verwijst naar een recent rapport van de Franse privacytoezichthouder CNIL, waarin wordt gesteld dat AI-modellen onder de GDPR kunnen vallen wanneer zij persoonsgegevens uit trainingsdata opslaan of “memoreren”.

Zal worden geëist dat overheidsdiensten systematisch re-identificatietests uitvoeren voor AI-modellen worden uitgerold, zoals de CNIL aanbeveelt?

De spreker benadrukt dat privacy ook geopolitiek is. Grote technologiebedrijven bezitten de belangrijkste communicatiekanalen, data en zelfs invloed op het publieke debat. Deze machtsconcentratie vormt een bedreiging voor de democratie.

Hij verwijst naar pleidooien voor controle over eigen data, interoperabiliteit en strengere controle op censuurmechanismen. Welke stappen worden gezet om data beter te verankeren in het kader van Europese soevereiniteit?

De Nederlandse Autoriteit Persoonsgegevens waar-schuwde recent dat vitale processen – zoals digitale identiteit en elektronisch verkeer met burgers – structureel afhankelijk zijn geworden van een beperkt aantal grote buitenlandse cloudproviders. Die afhankelijkheid vormt een reëel risico op maatschappelijke ontwrichting. De autoriteit stelt zelfs dat Nederland “tot stilstand kan komen” door grootschalige uitval of manipulatie. In België zal dit niet anders zijn.

De spreker verwijst naar het voorbeeld waarbij Amerikaanse sancties ertoe leidden dat medewerkers van het Internationaal Strafhof in Den Haag plots geen toegang meer hadden tot hun Microsoftmailbox.

Un mécanisme de contrôle parlementaire sera-t-il mis en place pour surveiller l'utilisation de l'IA par les services de sécurité?

En outre, l'intervenant demande comment la Belgique garantira que les systèmes d'IA utilisés par les pouvoirs publics, la police ou les administrations ne mémoriseront pas involontairement des données à caractère personnel, ce qui constituerait une violation du RGPD (Règlement général sur la protection des données). Il renvoie à un rapport récent de la CNIL, l'autorité française en charge de la protection des données, qui indique que les modèles d'IA peuvent relever du RGPD lorsqu'ils stockent ou “mémorisent” des données à caractère personnel provenant de données d'entraînement.

Les services publics seront-ils tenus d'effectuer systématiquement des tests de réidentification avant le déploiement de modèles d'IA, comme le recommande la CNIL?

L'intervenant souligne que la protection de la vie privée est également une question géopolitique. Les grandes entreprises technologiques détiennent les principaux canaux de communication ainsi que les données, et elles exercent même une certaine influence sur le débat public. Cette concentration du pouvoir constitue une menace pour la démocratie.

Il renvoie à certains plaidoyers en faveur du contrôle de ses propres données, de l'interopérabilité et d'une surveillance plus stricte des mécanismes de censure. Quelles mesures seront prises pour un meilleur ancrage des données dans le cadre de la souveraineté européenne?

L'Autorité néerlandaise de protection des données à caractère personnel a récemment mis en garde contre le fait que certains processus vitaux – tels que l'identité numérique et les communications électroniques avec les citoyens – sont devenus structurellement dépendants d'un nombre limité de grands fournisseurs de Cloud étrangers. Cette dépendance constitue un risque réel de perturbation sociale. L'autorité néerlandaise affirme même que les Pays-Bas “pourraient être paralysés” par une panne ou une manipulation à grande échelle. La situation ne sera pas différente en Belgique.

L'intervenant cite l'exemple des sanctions américaines qui ont soudainement privé des collaborateurs de la Cour pénale internationale à La Haye de l'accès à leur boîte mail Microsoft.

Welke concrete stappen zet België om vitale overheidsdata en communicatie minder afhankelijk te maken van niet-Europese cloudproviders?

De spreker verwijst naar de regelluwe experimenteerzones, een oud idee dat opnieuw in diverse beleidsnota's opduikt. Er wordt opnieuw een onderzoek aangekondigd naar mogelijke opportuniteiten. Hij vraagt om concrete duidelijkheid over wat hiervan in 2026 mag worden verwacht.

Daarnaast wijst hij op een element dat wel in de beleidsverklaring stond, maar ontbreekt in de beleidsnota: het aangekondigde samenwerkingsakkoord tussen de federale overheid, de GBA en de Vlaamse Toezichtcommissie. Hij vraagt of dit dossier stilgevallen is of elders wordt behandeld.

Tot slot verwijst de spreker naar een recent rapport van het Amerikaanse House of Representatives, getiteld *The Foreign Censorship Threat: Europe's Decade-Long Campaign to Censor the Global Internet and How It Harms American Speech in the United States*. Het rapport bevat zware kritiek op de uitvoering van de *Digital Services Act* (DSA) en op bredere Europese reguleringsinitiatieven, met belangrijke privacy-implicaties.

Hij vraagt om een eerste reactie op deze publicatie.

De heer Philippe Goffin (MR) wijst op de duidelijkheid en de samenhang van de beleidsnota. De beleidsnota geeft blijk van een evenwichtige en verantwoordelijke visie, in overeenstemming met het regeerakkoord, waarbij zowel het strategische karakter van gegevens als het fundamentele recht op bescherming van de privacy worden erkend. De gekozen aanpak lijkt resoluut pragmatisch: het bestaande evalueren, het juridische kader aanpassen, de samenwerking tussen de verschillende bestuursniveaus versterken en innovatie begeleiden met aandacht voor de essentiële waarborgen. Dat is precies wat het land nodig heeft in een context van versnelde digitale transformatie.

Het lid is met name verheugd dat de wet van 30 juli 2018 wordt geëvalueerd, dat de organieke wet van de Gegevensbeschermingsautoriteit wordt aangepast in overeenstemming met de constitutionele rechtspraak en dat ernaar wordt gestreefd het vertrouwen van de burgers te versterken bij de uitoefening van hun rechten. De bescherming van de privacy wordt niet voorgesteld als een remmende factor, maar als een hefboom voor legitimiteit en draagvlak voor het digitale beleid.

Quelles mesures concrètes la Belgique prend-elle pour réduire la dépendance des données publiques et communications vitales vis-à-vis des fournisseurs de Cloud non-européens?

L'intervenant fait référence aux zones d'expérimentation faiblement réglementées, une vieille idée qui refait surface dans diverses notes de politique générale. Une nouvelle étude sur de possibles opportunités est annoncée. Il demande des précisions concrètes sur ce que l'on peut s'attendre en 2026.

Il souligne également un élément qui figurait dans l'exposé d'orientation politique, mais qui n'est pas repris dans la note de politique générale: l'accord de coopération annoncé entre les pouvoirs publics fédéraux, l'Autorité de protection des données (APD) et la *Vlaamse toezichtcommissie* (VTC). Il demande si ce dossier est au point mort ou s'il sera traité ailleurs.

Enfin, l'intervenant fait référence à un rapport récent de la *House of Representatives* américaine, intitulé *"The Foreign Censorship Threat: Europe's Decade-Long Campaign to Censor the Global Internet and How It Harms American Speech in the United States"*. Ce rapport critique sévèrement la mise en œuvre du *Digital Service Act* ((DSA), la législation sur les services numériques aux États-Unis) et les initiatives réglementaires européennes plus larges, qui ont des implications importantes sur la protection de la vie privée.

Il demande une première réaction à cette publication.

M. Philippe Goffin (MR) souligne la clarté et la cohérence de la note de politique générale présentée. Celle-ci s'inscrit dans une vision équilibrée et responsable, conforme à l'accord de gouvernement, qui reconnaît à la fois le caractère stratégique des données et le droit fondamental à la protection de la vie privée. L'approche adoptée apparaît résolument pragmatique: évaluer l'existant, adapter le cadre juridique, renforcer la coopération entre niveaux de pouvoir et accompagner l'innovation sans renoncer aux garanties essentielles. C'est précisément ce dont le pays a besoin dans un contexte de transformation numérique accélérée.

Le membre se réjouit en particulier de l'évaluation de la loi du 30 juillet 2018, de l'adaptation de la loi organique de l'Autorité de protection des données dans le respect de la jurisprudence constitutionnelle, ainsi que de la volonté de renforcer la confiance des citoyens dans l'exercice de leurs droits. La protection de la vie privée n'est pas présentée comme un frein, mais comme un levier de légitimité et d'adhésion aux politiques numériques.

In de beleidsnota wordt er ook van uitgegaan dat gegevens onmisbaar zijn voor de werking van moderne overheden, wetenschappelijk onderzoek, innovatieve bedrijven en de ontwikkeling van artificiële intelligentie. De perspectieven op het gebied van experimenteerzones, gegevensbeheer en afstemming op Europese kaders zijn een positief signaal voor innovatie in België.

De spreker wijst vervolgens op een overkoepelende factor die bepalend is voor de doeltreffendheid van al die beleidsmaatregelen: de beveiliging van systemen en de weerbaarheid tegen cyberaanvallen. Het is begrijpelijk dat een beleidsnota die gericht is op privacy en gegevensbescherming niet in detail ingaat op hacking of cyberveiligheid in de strikte zin. Die materies vallen onder andere ministeriële bevoegdheden en onder specifieke operationele kaders en reeds bestaande regelingen op nationaal en Europees niveau. Naarmate gegevens echter meer worden gedeeld, systemen meer met elkaar worden verbonden en processen worden geautomatiseerd, wordt cyberbeveiliging een concrete voorwaarde voor de bescherming van de privacy.

Het vertrouwen van de burger – het kernthema van de beleidsnota – hangt niet alleen af van de kwaliteit van het rechtskader, maar ook van het vermogen van de Staat en de openbare instanties om illegale toegang tot gegevens te voorkomen, of het nu gaat om overheidsdiensten, gerechtelijke systemen, digitale platforms of innovatieve instrumenten die in experimentele omgevingen zijn ontwikkeld. Cyberaanvallen komen dagelijks veelvuldig voor en de getroffen personen staan vaak machteloos. De spreker vraagt hoe dat fenomeen in samenwerking met andere overheidsinstanties zal worden bestreden. Hij stipt aan dat een alomvattende aanpak noodzakelijk is.

Tot slot geeft hij aan dat zijn fractie de beleidsnota steunt. De nota is in overeenstemming met het regeerakkoord en streeft de daarin vastgelegde doelstellingen na.

De heer Pierre Jadoul (MR) wenst nadere informatie over verschillende punten en vraagt zich af wanneer er meer concrete informatie komt.

Een eerste aspect betreft de samenwerkingsovereenkomst tussen de Gegevensbeschermingsautoriteit en de Vlaamse Toezichtcommissie (VTC). Dat punt lijkt niet meer in de beleidsnota te staan. Hoe staat het met dat dossier? Zijn er onderhandelingen gaande, is het bijna afgerond, wordt het momenteel uitgevoerd of wordt het eventueel geschrapt?

Een tweede onderdeel betreft de administratieve vereenvoudiging. Het *only once*-principe, waar de beleidsnota naar verwijst, geniet brede steun, maar de

La note assume également que les données sont indispensables au fonctionnement des administrations modernes, à la recherche scientifique, aux entreprises innovantes et au développement de l'intelligence artificielle. Les perspectives ouvertes en matière de zones d'expérimentation, de gouvernance des données et d'articulation avec les cadres européens constituent un signal positif pour l'innovation en Belgique.

L'intervenant formule ensuite une observation concernant un élément transversal qui conditionne l'effectivité de l'ensemble de ces politiques: la sécurité des systèmes et la résilience face aux cyberattaques. Il est compréhensible qu'une note centrée sur la vie privée et la protection des données n'entre pas dans le détail du hacking ou de la cybersécurité au sens strict, ces matières relevant d'autres compétences ministérielles, de cadres opérationnels spécifiques et de dispositifs déjà existants aux niveaux national et européen. Toutefois, à mesure que les données sont davantage partagées, que les systèmes deviennent plus interconnectés et que les processus s'automatisent, la cybersécurité devient un préalable concret à la protection de la vie privée.

La confiance des citoyens – placée au cœur de la note – dépend non seulement de la qualité du cadre juridique, mais aussi de la capacité de l'État et des opérateurs publics à empêcher l'accès illégal aux données, qu'il s'agisse d'administrations, de systèmes judiciaires, de plateformes numériques ou d'outils innovants développés dans des environnements expérimentaux. Les cyberattaques sont nombreuses et quotidiennes, et les personnes touchées se retrouvent souvent démunies. L'intervenant demande comment ce phénomène sera combattu en coordination avec les autres niveaux de pouvoir et souligne la nécessité d'une approche globale.

Pour conclure, il indique que son groupe soutient la note de politique générale: elle est conforme à l'accord de gouvernement et poursuit les objectifs qui y sont fixés.

M. Pierre Jadoul (MR) souhaite obtenir des précisions sur plusieurs points et s'interroge sur l'échéance à laquelle des éléments plus concrets pourront être communiqués.

Un premier aspect concerne l'accord de coopération entre l'Autorité de protection des données et la *Vlaamse Toezichtcommissie* (VTC). Ce point ne semble plus figurer dans la note de politique générale. Quel est l'état d'avancement de ce dossier: négociation en cours, finalisation, mise en œuvre, ou éventuel abandon?

Un deuxième volet porte sur la simplification administrative. Le principe du *"only once"*, rappelé dans la note, bénéficie d'un large soutien, mais sa mise en

uitvoering ervan blijft complex. Hoe zal dat principe concreet worden omgezet in de praktijk en wanneer kan redelijkerwijs een eerste ontwerp voor vereenvoudiging worden verwacht?

Een derde dossier betreft de toegang van onderzoekers tot gerechtelijke dossiers, zowel strafrechtelijke als burgerrechtelijke. In de beleidsnota wordt verwezen naar overleg met het College van procureurs-generaal en met de hoven en rechtbanken. Het lid wenst meer details over die gesprekken. Hij wil ook graag weten wanneer academici daadwerkelijk gereguleerde toegang tot die gegevens krijgen.

Ten slotte gaat de spreker in op de regulering van sociale media. Op basis van een voorstel van resolutie vinden momenteel hoorzittingen plaats in de commissie voor Justitie. Kan de minister een indicatieve tijdlijn geven? Dat project kan weliswaar niet op enkele weken worden afgehandeld, maar het totale gebrek aan deadlines dreigt elke vooruitgang te belemmeren. Het zou nuttig zijn te weten welke stappen kunnen worden overwogen, rekening houdend met het feit dat het tijdspad niet alleen van België maar ook van Europa afhangt. Het lid vraagt zich af hoe de besprekingen op EU-niveau verlopen, hoever Frankrijk op dat vlak is gevorderd, of Frankrijk van plan is zijn model aan andere lidstaten op te leggen en wat het standpunt van de minister ter zake is.

De heer Khalil Aouasti (PS) wijst op het belang van het fundamentele en door en door individuele recht op privacy. In tijden waarin digitale technologieën almaar meer verweven raken met eenieders dagelijkse realiteit, hebben tal van burgers – gezinnen, jongeren, ouderen, kwetsbare personen of mensen met een fysieke of mentale aandoening – behoefte aan begeleiding, advies en bescherming. Van de overheid verwachten zij dat die haar regulerende rol ten volle opneemt door grenzen te stellen, een kader te scheppen voor vaak indringende technologieën en te waarborgen dat de persoonlijke levenssfeer wordt beschermd.

De verwachtingen zijn hooggespannen, want het gebruik van persoonsgegevens groeit en de bijbehorende risico's nemen toe. De overheden dragen een collectieve verantwoordelijkheid ten aanzien van technologische ontwikkelingen die de traditionele regelgeving in snelheid nemen.

Net op dat vlak maakt de spreker zich grote zorgen. De beleidsnota accentueert een verschuiving die al tijdens de vorige legislatuur merkbaar was, met name dat privacy minder wordt gezien als een structuurgevend grondrecht en meer als een instrument voor economische ontwikkeling. De nota is doorweven van een logica die

œuvre demeure complexe. Comment ce principe sera-t-il concrètement traduit dans les faits et à quel horizon une première ébauche de simplification pourrait raisonnablement être envisagée?

Un troisième dossier concerne l'accès des chercheurs aux dossiers judiciaires, tant pénaux que civils. La note mentionne des concertations avec le Collège des procureurs généraux ainsi qu'avec les cours et tribunaux. Le membre souhaite obtenir davantage de précisions sur ces échanges et sur le moment où les milieux académiques pourront effectivement bénéficier d'un accès encadré à ces données.

Enfin, l'intervenant aborde la question de la régulation des réseaux sociaux. Des auditions sont en cours en commission de la Justice sur la base d'une proposition de résolution. La ministre peut-elle annoncer une ligne du temps indicative. Même si ce chantier ne se réglera pas en quelques semaines, l'absence totale d'échéances risque de freiner toute avancée. Il serait utile de savoir quelles étapes peuvent être envisagées, en tenant compte du fait que le calendrier n'est pas uniquement belge mais également européen. Le membre s'interroge sur l'état des discussions au niveau de l'Union, sur l'avancement de la France dans ce domaine, sur la volonté éventuelle de celle-ci d'imposer son modèle aux autres États membres, ainsi que sur la position de la ministre à cet égard.

M. Khalil Aouasti (PS) rappelle l'importance du droit à la vie privée, droit fondamental et profondément individuel. Dans un contexte où le numérique traverse désormais le quotidien de tout le monde, de nombreux citoyens – familles, jeunes, personnes âgées, personnes vulnérables ou en situation de fragilité physique ou mentale – ont besoin d'être accompagnés, conseillés et protégés. Ce qu'ils attendent des pouvoirs publics, c'est qu'ils assument pleinement leur rôle régulateur: fixer des limites, encadrer des technologies parfois intrusives et garantir que ce qui relève de l'intime demeure protégé.

Les attentes sont élevées, car l'usage des données personnelles s'intensifie et les risques augmentent. Les pouvoirs publics ont une responsabilité collective face à des évolutions technologiques qui ont largement dépassé les cadres traditionnels de régulation.

C'est précisément sur ce point que l'intervenant exprime une préoccupation majeure. La note de politique générale accentue une inflexion déjà perceptible sous la précédente législature: la vie privée y apparaît moins comme un droit fondamental structurant que comme un instrument au service du développement économique.

innovatie, concurrentiekracht en economische noodzaak lijkt te doen primeren op gegevensveiligheid. Die benadering houdt een heus risico in, namelijk dat de burgers, als rechtssubjecten, veeleer worden beschouwd als gebruikers van digitale diensten en bezitters van nuttige gegevens dan als houders van grondrechten waarover ze meester moeten blijven.

Die al bestaande trend lijkt zich in de beleidsnota nog scherper af te tekenen. Dat is zorgwekkend, gezien de snelheid van digitale ontwikkelingen en de uitdijende kloof tussen de macht van de platformen en de slagkracht van overheden. Al te vaak wordt gezwaaid met het argument dat alles op Europees niveau moet worden beslist, maar bij nieuwe uitdagingen kan aldus niet kort genoeg op de bal worden gespeeld.

De spreker wijst ook op de hardnekkige wanverhouding tussen de macht van de grote platformen, de beperkte capaciteiten van de kmo's en zkm's en de rechten van de burgers. Hij betreurt dat er geen gedifferentieerde impactanalyses per doelgroep zijn uitgevoerd, terwijl de effecten van nieuwe technologieën verschillen naargelang van de bevolkingsgroep.

De heer Aouasti formuleert een eerste vraag voor het hele Parlement en in het bijzonder voor de meerderheid. Hij wijst op de inconsistentie tussen de ambitie in de beleidsnota en de middelen die de Gegevensbeschermingsautoriteit worden toebedeeld. De GBA krijgt er immers almaar meer opdrachten bij – AVG, artificiële intelligentie, de *Data Act*, de *Data Governance Act*, experimenteeromgevingen (*sandboxes*), Europese samenwerking – en toch is de meerderheid niet ingegaan op haar vraag om extra budget.

Het klopt dat de minister geen voorgedij heeft over de GBA en dus niet beslist over de begroting ervan. Dat is de verantwoordelijkheid van het Parlement, maar laat de meerderheid daar nu net ook deel van uitmaken. Die tegenstrijdigheid ondermijnt het vermogen van de GBA om al haar taken naar behoren te vervullen. Er is duidelijk een discrepantie tussen de regeringsambities op het vlak van gegevensbescherming en de budgettaire omzetting van diezelfde ambities door de meerderheid in het Parlement. Hoewel de GBA voortdurend schreeuwt om extra middelen omdat haar takenpakket maar blijft uitbreiden, krijgt ze die dus niet.

Vervolgens staat de spreker stil bij de evaluatie van het COC. In de beleidsnota staat te lezen dat de minister bij de Kamer een verzoek heeft ingediend om de werking van het COC te laten doorlichten door het Rekenhof. Aangezien het COC een onafhankelijk orgaan is verbonden aan het Parlement, is de minister niet rechtstreeks verantwoordelijk

La note est traversée par une logique où l'innovation, la compétitivité et les impératifs économiques semblent primer sur la protection des données. Le membre estime que cette orientation présente un risque réel: les citoyens, sujets de droit, tendent à être envisagés davantage comme utilisateurs de services numériques et détenteurs de données exploitables que comme titulaires de droits fondamentaux dont ils doivent rester maîtres.

Cette inflexion, déjà existante, semble s'accroître dans la note, ce qui est préoccupant au regard de la rapidité des évolutions numériques et du décalage croissant entre la puissance des plateformes et la capacité d'action des pouvoirs publics. L'argument selon lequel "tout doit se décider au niveau européen" est trop souvent invoqué et insuffisant pour répondre aux enjeux immédiats.

L'intervenant relève également une asymétrie persistante entre le pouvoir des grandes plateformes, les capacités limitées des PME et TPE, et les droits des citoyens. Il regrette l'absence d'analyses d'impact différenciées selon les publics concernés, alors que les effets des technologies ne touchent pas toutes les catégories de la population de la même manière.

Le membre formule une première question, adressée à l'ensemble du Parlement et en particulier à la majorité. Il souligne une incohérence entre l'ambition affichée dans la note et les moyens alloués à l'Autorité de protection des données. Les missions du régulateur ne cessent de s'étendre – RGPD, intelligence artificielle, *Data Act*, *Data Governance Act*, *sandboxes*, coopération européenne – alors que la majorité parlementaire a refusé d'accorder les moyens budgétaires supplémentaires demandés par l'APD.

Le membre rappelle que la ministre n'a pas la tutelle sur l'APD et ne décide pas de son budget, mais que la responsabilité incombe au Parlement, dont la majorité fait partie. Il estime que cette contradiction fragilise la capacité du régulateur à exercer pleinement son rôle. Il y a là une incohérence importante au sein de la majorité entre les ambitions affichées par le gouvernement en matière de protection des données et la traduction budgétaire de ces ambitions par cette même majorité au Parlement. Alors même que l'Autorité régulatrice signale l'extension continue de ses missions et la nécessité de moyens supplémentaires, ces moyens lui sont refusés.

Un autre point concerne l'évaluation du COC. La note de politique générale indique qu'une demande d'évaluation a été adressée à la Chambre pour solliciter l'intervention de la Cour des comptes. Le COC étant un organe indépendant relevant du Parlement, cette démarche ne dépend pas directement de la ministre.

voor die evaluatie. Volgens de heer Auousti is dat verzoek evenwel niet besproken in de commissie. Dat roept heel wat vragen op. Bestaat er misschien een tijdpad dat al aan de regering is meegedeeld maar nog niet aan het Parlement? Welke termijn heeft men voor ogen voor de indiening van een resolutie om die evaluatie mogelijk te maken? Hoe zal die evaluatie in haar werk gaan? Zal ze uitsluitend worden toevertrouwd aan het Rekenhof of zal aanvullend technisch advies worden ingewonnen inzake gegevensbescherming en parlementaire zowel als gerechtelijke procedurele waarborgen? Het COC is immers nog steeds een onafhankelijk orgaan dat onder het begrotingstoezicht van het Parlement staat.

De spreker wijst voorts op een element dat in de beleidsnota aan bod komt maar niet in de commissie werd besproken: het bestaan van een brief aan het Parlement. Hij is daar niet van op de hoogte en zou willen weten waar die brief zich bevindt.

Met betrekking tot het CSAM-dossier wil de spreker vernemen welke belangrijke punten nog onderwerp van discussie zijn tussen de instellingen en binnen welke termijn een uitkomst kan worden verwacht, onder meer in verband met de debatten over de resolutie die al enkele weken lopen in het Parlement.

Wat de bescherming van minderjarigen op platforms betreft, verwijst de beleidsnota naar de werkzaamheden van de commissie voor Justitie, aangevat naar aanleiding van de resolutie van een collega. Volgens de spreker vertoont de beleidsnota echter een tekortkoming: minderjarigen komen erin aan bod, maar enkel vanuit controleoogpunt, zonder een meer omvattende dimensie van emancipatie, vorming of autonomie. Er wordt niets gezegd over digitale geletterdheid, noch over investeringen in preventie of vormingen rond mediawijsheid. Wordt in het kader van de aangekondigde contacten met de deelstaten aandacht besteed aan de volledige keten – preventie, educatie, autonomie, bescherming – of enkel aan het aspect controle? Het lid herinnert eraan dat de meeste gehoorde actoren, vooral zij die instaan voor de bescherming van minderjarigen, terughoudend waren ten aanzien van een op leeftijd gebaseerd toegangsverbod. Zij beschouwen dat als ineffectief of in strijd met de rechten van jongeren.

De vraag luidt dus: welke koers beoogt men te varen? Wil men een verbod of een leeftijdsgebonden toegangsbeperking? De spreker vraagt zich ook af of men op Belgisch niveau actie kan ondernemen zonder de Europese ontwikkelingen te volgen, zeker als men bedenkt dat dit thema in het Europese deel van de beleidsnota wordt behandeld en niet in het nationale deel.

Toutefois, à la connaissance de l'intervenant, cette demande n'a pas été discutée en commission. La question porte donc sur l'existence éventuelle d'un calendrier communiqué à l'exécutif mais non encore partagé avec les parlementaires, sur le délai envisagé pour le dépôt d'une résolution permettant cette évaluation, ainsi que sur la nature de l'évaluation elle-même: sera-t-elle confiée exclusivement à la Cour des comptes ou complétée par d'autres expertises, notamment techniques, portant sur la protection des données et les garanties procédurales, qu'elles soient parlementaires ou judiciaires? Le COC demeure en effet un organisme indépendant placé sous la tutelle budgétaire du Parlement.

L'intervenant relève également un élément mentionné dans la note mais non discuté en commission: l'existence d'un courrier adressé au Parlement, dont il n'a pas connaissance, et dont il souhaiterait savoir où il se trouve.

S'agissant du dossier CSAM, l'intervenant souhaite connaître les principaux points encore en discussion entre les institutions et l'horizon dans lequel un aboutissement pourrait être envisagé, notamment en lien avec les débats en cours sur la résolution examinée depuis plusieurs semaines au Parlement.

Concernant la protection des mineurs sur les plateformes, la note renvoie aux travaux de la commission Justice entamés sur la base de la résolution d'un collègue. L'intervenant estime toutefois que la note présente une faiblesse: les mineurs n'y apparaissent que sous l'angle du contrôle, sans dimension plus globale d'émancipation, de formation ou d'autonomie. Aucune mention n'est faite de l'éducation numérique, ni d'investissements en matière de prévention ou d'éducation critique au numérique. Dans le cadre des contacts annoncés avec les entités fédérées, l'ensemble de la chaîne – prévention, éducation, autonomie, protection – est-il abordé, ou seul le volet contrôle est-il traité? Le membre rappelle que la plupart des acteurs auditionnés, notamment ceux chargés de la protection des mineurs, se sont montrés réticents à une interdiction d'accès fondée sur l'âge, jugée inefficace ou attentatoire aux droits des jeunes.

La question porte donc sur l'orientation envisagée: interdiction ou limitation d'accès en fonction de l'âge? Et sur la capacité d'agir au niveau belge, indépendamment des développements européens, alors que la thématique figure dans la partie européenne de la note et non dans la partie nationale.

De spreker merkt vervolgens op dat de beleidsnota geen melding meer maakt van het opheffen van de anonimiteit online. Enkel de kwestie van de leeftijds-grens op sociale media komt aan bod. Nochtans is de mogelijkheid om de anonimiteit snel en doeltreffend op te heffen een centraal aspect in de besproken resolutie en andere parallel behandelde teksten. Het ontbreken van dit thema in de beleidsnota roept vragen op: is het geen prioriteit, is het een vergetelheid of is het een element dat samen met andere maatregelen moet worden behandeld?

Wat de regelluwe zones betreft, die al in de vorige beleidsnota aan bod kwamen en gelinkt zijn aan diverse *sandboxes*, wenst de spreker opheldering. Het draait erom te bepalen of die zones bepaalde bedrijven de mogelijkheid zouden bieden om in het belang van de economische ontwikkeling gedeeltelijk af te wijken van de bescherming van persoonsgegevens. Anders gesteld: kan worden afgeweken van het recht op privacy? Hij vraagt zich ook af of dergelijke afwijkingen wel verenigbaar zijn met het huidige rechtskader, met name de AVG, en of een tijdelijke opschorting van grondrechten kan worden gerechtvaardigd in naam van innovatie.

De spreker wil vernemen of er expliciete uittredingsmechanismen bestaan en welke onafhankelijke evaluatie- of sanctiemechanismen er zijn om eventuele uitwassen te voorkomen of te corrigeren.

De beleidsnota verwijst naar een studie van de FOD Economie; het zou nuttig zijn de conclusies daarvan te kennen, opdat het parlementair debat kan plaatsvinden met volledige kennis van zaken.

De beleidsnota verwijst tevens naar het omnibusakkoord dat op 16 december 2025 door het Europees Parlement werd aangenomen en door tal van actoren inzake gegevensbescherming wordt beschouwd als een verzwakking van de AVG die indruist tegen de initiële doelstelling, namelijk een consolidatie van de rechten. De spreker wil vernemen wat de regering vindt over die als een achteruitgang aangevoelde evolutie. Moeten we ons aan het nieuwe Europese kader aanpassen of onze meer beschermende nationale wetgeving in stand houden?

Tot slot wijst hij op een vorm van Europese strategie die hij als “volgzaam” omschrijft: de vraag is of het Belgische standpunt beperkt zal blijven tot de ondersteuning van het bestaande Europese kader, dan wel of België op Europees niveau net een beschermingsniveau wil verdedigen dat is afgestemd op zijn eigen, strengere wetgeving.

L'intervenant observe ensuite que la note ne mentionne plus la levée de l'anonymat en ligne. Seule la question de la limite d'âge sur les réseaux est abordée. Pourtant, dans le cadre de la résolution discutée et d'autres textes examinés en parallèle, la capacité de lever rapidement et efficacement l'anonymat constitue un enjeu central. L'absence de cette thématique dans la note interpelle: s'agit-il d'une non-priorité, d'un oubli ou d'un élément appelé à être traité conjointement avec d'autres mesures?

En ce qui concerne les zones faiblement réglementées, déjà évoquées dans la précédente note de politique générale et associées à diverses *sandboxes*, l'intervenant souhaite une clarification. Il s'agit de déterminer si ces zones permettraient à certaines entreprises de déroger partiellement à la protection des données personnelles au nom du développement économique, et donc de savoir s'il est question de dérogations au droit à la vie privée. La question porte également sur la compatibilité de telles dérogations avec le cadre juridique actuel, notamment le RGPD, et sur la justification d'une suspension temporaire de droits fondamentaux au nom de l'innovation.

L'intervenant souhaite connaître l'existence éventuelle de mécanismes explicites de sortie, ainsi que les mécanismes d'évaluation indépendants ou de sanction prévus pour prévenir ou corriger toute dérive.

La note évoque une étude du SPF Économie; il serait utile d'en connaître les conclusions afin de permettre un débat pleinement éclairé au Parlement.

La note mentionne également l'accord Omnibus adopté au Parlement européen le 16 décembre 2025, présenté par de nombreux acteurs de la protection des données comme un affaiblissement du RGPD, allant à rebours de l'objectif initial de consolidation des droits. L'intervenant souhaite connaître la position du gouvernement sur ce qui est perçu comme un recul: adaptation au nouveau cadre européen ou maintien d'un droit national plus protecteur?

Il relève enfin une forme de stratégie européenne qu'il qualifie de “suiviste”: la question est de savoir si la position belge se limitera à accompagner le cadre européen existant ou si, au contraire, la Belgique entend défendre, au niveau européen, un niveau de protection aligné sur son propre droit, plus exigeant.

Tot slot verwijst de spreker naar Conventie 108 van de Raad van Europa, geamendeerd bij Conventie 223 maar nog steeds niet door België geratificeerd. Wat is het tijdspad van de regering voor die ratificatie?

De heer Ismaël Nuino (Les Engagés) is blij met het in deze aangelegenheid verrichte werk. Hij benadrukt dat we geneigd zouden kunnen zijn privacy als een tweederangsonderwerp te beschouwen. Nochtans is privacy gaandeweg steeds belangrijker geworden.

De overheid dient er inderdaad terdege rekening mee te houden bij het toezicht op persoonsgegevens en de verzameling en het gebruik ervan. Voor de bedrijven zijn persoonsgegevens een strategisch middel, te vergelijken met een hoogwaardige grondstof die moet kunnen worden verwerkt en geëxploiteerd, in casu via krachtige algoritmen.

Die economische waarde van persoonsgegevens creëert een spanningsveld tussen Staat, burgers en bedrijven, want die gegevens kunnen aanzienlijke winsten genereren en vereisen een doelmatige overheidsregulering. Voor burgers gaat het om hun privéleven, hun gewoonten, hun keuzes, om wat ze wel of niet doen. Uit de recente debatten in de commissie voor Justitie over met name anonimiteit online blijkt dat bedrijven zoals Meta over miljoenen gegevens van hun gebruikers beschikken, die op gewoon verzoek toegankelijk zijn. Persoonsgegevens winnen dus aan belang en die tendens zal zich voortzetten.

Het stemt de spreker tevreden dat het onderwerp niet alleen in de beleidsnota van de minister, maar ook in haar dagelijks beleid prioriteit krijgt. De heer Nuino vindt het positief dat de minister het vertrouwen van de burgers in de overheidsadministraties en in de Staat wil versterken op het vlak van het beheer van hun persoonsgegevens. Hij benadrukt ook de aandacht die in de beleidsnota gaat naar een evenwicht tussen innovatie en grondrechten; dat evenwicht is noodzakelijk, willen we bedrijven kansen geven om te innoveren en tegelijkertijd onze Europese waarden veiligstellen. Europa moet zijn digitale soevereiniteit behouden; bedrijven dienen dan ook perspectieven te krijgen, zonder dat aan de eerbiediging van de grondrechten wordt getornd.

Een ander belangrijk en door verscheidene collega's aangehaald punt betreft de bescherming van jongeren wanneer ze online zijn. De recente hoorzittingen over onlineanonimiteit en leeftijdsverificatie waren bijzonder leerzaam en legden de uitdagingen, moeilijkheden en valkuilen ter zake bloot.

En conclusion, l'intervenant évoque la Convention 108 du Conseil de l'Europe, amendée par le traité 223 mais toujours non ratifiée par la Belgique. Quel est le calendrier prévu par le gouvernement pour procéder à cette ratification?

M. Ismaël Nuino (Les Engagés) salue le travail réalisé dans ce domaine. Il souligne que l'on pourrait être tenté de considérer la vie privée comme un sujet secondaire. Pourtant, au fil du temps, cette matière s'impose comme un enjeu de plus en plus central.

La question de la vie privée devient en effet essentielle pour l'État sous l'angle du contrôle des données personnelles et de la collecte ou de l'usage qui en est fait. Pour les entreprises, les données personnelles constituent une ressource stratégique, comparable à une matière première de grande valeur, qu'il faut être capable de traiter et d'exploiter, notamment via des algorithmes performants.

Cette valeur économique crée une tension entre l'État, les citoyens et les entreprises, car les données permettent de générer des profits importants et nécessitent une régulation publique efficace. Pour les citoyens, il s'agit de leur vie privée, de leurs habitudes, de leurs choix, de ce qu'ils décident de faire ou de ne pas faire. Les débats récents en commission de la Justice, notamment sur l'anonymat en ligne, ont montré que des entreprises comme Meta disposent de millions d'informations sur leurs utilisateurs, accessibles sur simple demande. Les données personnelles deviennent ainsi un enjeu croissant, appelé à prendre encore davantage d'importance.

L'intervenant se réjouit que ce sujet soit traité comme une priorité, non seulement dans la note de politique générale, mais aussi dans la politique quotidienne menée par la ministre. Il salue la volonté de renforcer la confiance des citoyens dans les administrations publiques et dans l'État quant à la gestion de leurs données personnelles. Il souligne également l'attention portée à l'équilibre entre innovation et droits fondamentaux, équilibre essentiel pour permettre aux entreprises d'innover tout en préservant les valeurs européennes. L'Europe doit maintenir sa souveraineté numérique, ce qui implique d'ouvrir des perspectives aux entreprises tout en garantissant le respect des droits fondamentaux.

Un autre point important concerne la protection des jeunes en ligne, largement évoquée par plusieurs collègues. Les auditions menées récemment sur l'anonymat en ligne et la vérification de l'âge ont été particulièrement instructives, révélant les enjeux, les difficultés et les écueils à surmonter.

Media-educatie is uitvoerig aan bod gekomen, hoewel de heer Nuino eraan herinnert dat dit, gelet op de Belgische institutionele structuur, geen federale bevoegdheid is. Hij benadrukt dat er interferedele overeenkomsten moeten komen om een doelmatige afstemming tussen de verschillende bestuursniveaus te garanderen, al erkent hij dat elk institutioneel niveau de eigen bevoegdheden ter zake moet uitoefenen.

Het debat over anonimiteit online en leeftijdscontrole zal nog niet onmiddellijk worden beslecht. Tijdens de hoorzittingen kunnen aanbevelingen worden geformuleerd en eenmaal concrete voorstellen op tafel zal een diepgaand debat kunnen plaatsvinden.

Fragmentatie is een ander element dat door verschillende sprekers werd aangebracht: sommige actoren hebben benadrukt dat nationale of Europese regels op gespannen voet kunnen komen te staan met de verificatiesystemen die de grote bedrijven reeds hebben ingevoerd. Toch is het legitiem dat België en de Europese Unie hun eigen regels opstellen en privébedrijven verplichten die na te leven. De vraag in hoeverre die gemeenschappelijke regels kunnen worden afgedwongen is dan ook cruciaal, vooral ten aanzien van mondiale bedrijven die niet enkel door de nationale normen gebonden zijn. De *Digital Services Act* is een essentieel instrument in dat verband; die verordening is immers een waarborg voor de Europese soevereiniteit en de naleving van de Europese wetgeving.

De heer Nuino gaat ook in op iets praktisch dat tijdens de hoorzittingen naar voren kwam: volgens sommige deskundigen zou de itsme-toepassing niet toegankelijk zijn voor jongeren onder de 16 jaar. Welke ontwikkelingen staan er dienaangaande op stapel en wat valt de komende maanden of jaren te verwachten?

Tot slot staat de heer Nuino stil bij artificiële intelligentie, die een steeds grotere plaats in ons dagelijks leven inneemt. Hij verwijst daarbij naar een nieuw sociaal medium dat enkel voor interacties tussen algoritmes bedoeld is. Hij vraagt zich af waar het met de gegevensverwerking naartoe moet in het AI-tijdperk, aangezien AI-systemen met enorme hoeveelheden gegevens, waaronder die van gebruikers, worden gevoed ter verbetering van hun modellen. Hij haalt er het voorbeeld bij van Meta, waarvan het AI-systeem de gegevens van Belgische burgers verwerkt. Waar worden die gegevens en gegevensstromen fysiek opgeslagen en met welke privacywaarborgen?

Ter afronding van zijn betoog wijst de heer Nuino erop dat privacykwesties voor zowel de bedrijven als de burgers steeds belangrijker worden. Hij benadrukt dat de beleidsverantwoordelijken een duidelijke visie

L'éducation aux médias a été largement évoquée, mais l'intervenant rappelle que, du fait de la structure institutionnelle belge, cette compétence ne relève pas du niveau fédéral. Il souligne la nécessité d'accords interfédéraux pour assurer une coordination efficace entre les différents niveaux de pouvoir, tout en reconnaissant que chacun doit exercer ses compétences dans le cadre qui lui est propre.

Le débat sur l'anonymat en ligne et la vérification de l'âge n'a pas vocation à être tranché immédiatement. Les auditions permettront de formuler des recommandations, et un débat approfondi pourra être mené lorsque des propositions concrètes seront présentées.

Un autre élément soulevé par plusieurs intervenants concerne la fragmentation: certains acteurs ont souligné que des règles nationales ou européennes pourraient entrer en tension avec les systèmes de vérification déjà mis en place par les grandes entreprises. Il est néanmoins légitime que la Belgique et l'Union européenne définissent leurs propres règles et obligent les entreprises privées à s'y conformer. La question centrale devient alors celle de la capacité à faire respecter ces règles communes, notamment face à des entreprises mondiales qui ne se limitent pas aux normes nationales. Le DSA constitue un outil essentiel à cet égard, visant à garantir la souveraineté européenne et le respect des lois européennes.

L'intervenant souhaite également aborder une question pratique soulevée lors des auditions: certains experts ont indiqué que l'application Itsme n'était pas accessible aux moins de 16 ans. Il serait utile de connaître les évolutions éventuelles dans ce domaine et les perspectives pour les mois ou années à venir.

Enfin, l'intelligence artificielle occupe une place croissante dans la vie quotidienne. L'intervenant évoque même l'apparition récente d'un réseau social où seules des intelligences artificielles interagissent entre elles. Il s'interroge sur l'évolution du traitement des données dans le cadre de l'IA, sachant que ces systèmes se nourrissent de grandes quantités de données, y compris celles fournies par les utilisateurs, pour améliorer leurs modèles. Il cite l'exemple de Meta, dont l'intelligence artificielle traite des données de citoyens belges, et s'interroge sur la localisation des flux et du stockage de ces données, ainsi que sur les garanties offertes quant au respect de la vie privée.

En conclusion, l'intervenant rappelle que les enjeux liés à la vie privée deviennent de plus en plus importants, tant pour les entreprises que pour les citoyens. Il souligne la nécessité, pour les responsables politiques,

moeten ontwikkelen over de te verdedigen waarden en de limieten die aan privéactoren moeten worden opgelegd, wil men komen tot een ecosysteem dat de privacy respecteert.

Mevrouw Nele Daenen (Vooruit) beklemtoont dat privacy geen luxe is en ook geen rem op vooruitgang vormt, maar een fundamenteel recht en tegelijk een noodzakelijke voorwaarde om mensen mee te nemen in de digitale toekomst. In een samenleving waarin data steeds meer bepalen hoe wordt gewerkt, geleerd, gezorgd en gecommuniceerd, is het cruciaal dat burgers vertrouwen hebben dat hun gegevens correct worden gebruikt, niet misbruikt worden en niet zonder noodzaak worden verzameld. De beleidsnota erkent terecht het evenwicht tussen innovatie en bescherming, tussen efficiënt bestuur en fundamentele rechten. Tegelijk blijven er voor Vooruit enkele belangrijke aandachtspunten.

De minister kondigt een nieuwe evaluatie aan van de wet van 30 juli 2018 en mogelijke aanpassingen aan de Gegevensbeschermingsautoriteit. Hoe zal ze garanderen dat deze evaluatie niet louter technisch, maar ook maatschappelijk gedragen is? Worden vakbonden, middenveldorganisaties, privacyexperten en burgerrechtenorganisaties structureel betrokken?

Kan de minister bevestigen dat eventuele hervormingen van de GBA haar onafhankelijkheid niet ondergraven, maar net versterken?

Het *only once*-principe kan administratieve lasten verminderen, wat Vooruit volmondig ondersteunt. Tegelijk mag vereenvoudiging nooit uitmonden in datamassificatie. Hoe voorkomt de minister dat burgers het gevoel krijgen dat “de overheid alles van hen weet, overal en altijd”? Komt er één duidelijke, transparante inzage voor burgers in wie hun gegevens gebruikt, waarom en hoelang?

Wat de regelluwe experimenteerzones betreft, erkent de spreker het belang van innovatie en het ondersteunen van start-ups, kmo's en onderzoek. Hoe zorgt de minister ervoor dat regelluwe experimenteerzones geen “privacyvrije zones” worden? Zal elke experimenteerzone verplicht vooraf een impactanalyse op grondrechten uitvoeren, met bijzondere aandacht voor kwetsbare

de tracer une vision claire des valeurs à défendre et des balises à imposer aux acteurs privés afin de garantir un écosystème respectueux de la vie privée.

Mme Nele Daenen (Vooruit) souligne que la vie privée n'est ni un luxe ni un frein au progrès, mais un droit fondamental et une condition nécessaire pour accompagner les citoyens dans l'avenir numérique. Dans une société où les données déterminent de plus en plus la manière dont nous travaillons, apprenons, prenons soin des autres et communiquons, il est crucial que les citoyens aient confiance dans le fait que leurs données sont utilisées correctement, ne sont pas exploitées à mauvais escient et ne sont pas collectées sans nécessité. La note de politique générale reconnaît à juste titre l'équilibre entre innovation et protection, entre administration efficace et droits fondamentaux. Vooruit estime toutefois qu'il convient de rester attentif à certains points importants.

La ministre annonce une nouvelle évaluation de la loi du 30 juillet 2018 et d'éventuelles modifications à apporter à la loi portant création de l'Autorité de protection des données. Comment garantira-t-elle que cette évaluation ne sera pas purement technique, mais qu'elle bénéficiera également d'un soutien de la société? Les syndicats, les organisations de la société civile, les experts en matière de protection de la vie privée et les organisations de défense des droits civils seront-ils associés de manière structurelle?

La ministre peut-elle confirmer que les éventuelles réformes relatives à l'APD ne porteront pas préjudice à son indépendance mais, au contraire, viseront à la renforcer?

Le principe *only once* peut permettre de réduire la charge administrative, ce que Vooruit soutient sans réserve. La simplification ne doit toutefois jamais entraîner une massification des données. Comment la ministre compte-t-elle éviter que les citoyens aient le sentiment que les autorités savent tout sur eux, partout et à tout moment? Les citoyens disposeront-ils d'un accès clair et transparent aux informations concernant les utilisateurs de leurs données, les raisons de cette utilisation et sa durée?

En ce qui concerne les zones d'expérimentation faiblement réglementées, l'intervenante reconnaît l'importance de l'innovation et du soutien aux start-ups, aux PME et à la recherche. Comment la ministre veille-t-elle à ce que les zones d'expérimentation faiblement réglementées ne deviennent pas des “zones sans vie privée”? Chaque zone d'expérimentation sera-t-elle tenue de

groepen? Innovatie die mensen wantrouwig maakt, is geen vooruitgang. Geen innovatie zonder vertrouwen.

De bescherming van kinderen online blijft een prioriteit. De aandacht van de minister voor CSAM, de DSA en leeftijdsverificatie is terecht, maar het evenwicht is uiterst gevoelig. Hoe vermijdt de minister dat leeftijdsverificatie leidt tot extra dataverzameling of indirecte surveillance? Zal België expliciet inzetten op privacyvriendelijke oplossingen, zoals anonieme of lokale verificatiemodellen?

De minister erkent terecht dat politie en inlichtingendiensten moderne middelen nodig hebben, maar net daar is democratische controle cruciaal. Hoe verzekert de minister dat AI-toepassingen in opsporing niet leiden tot discriminatie of profilering? Wordt het Parlement systematisch geïnformeerd over nieuwe toepassingen in experimentele contexten?

De heer Steven Matheï (cd&v) constateert dat de beleidsnota duidelijk maakt dat privacy een belangrijk thema is, wat zich ook weerspiegelt in verschillende maatschappelijke debatten. De nota is opgebouwd rond een nationaal en internationaal kader, waarbij meteen een evaluatie wordt aangekondigd. Tegelijk blijft de klassieke evenwichtsoefening bestaan tussen enerzijds privacy en de bescherming van persoonsgegevens en anderzijds de ontwikkeling van initiatieven die die gegevens onder druk kunnen zetten.

Bij de aangekondigde evaluatie merkt de spreker op dat dit een goede zaak is. De GDPR-regels en de Belgische privacywetgeving dateren van 2018, terwijl de ontwikkelingen sindsdien snel zijn gegaan. Evalueren en de vinger aan de pols houden is dus noodzakelijk.

Met betrekking tot het internationaal niveau stelt de spreker de vraag naar de stand van zaken, onder meer inzake de digitale omnibus en de vertaling daarvan naar het federale niveau.

Ook op nationaal vlak zijn er vragen. De GBA blijft een belangrijke actor in het privacylandschap, waar het afgelopen jaar veel is gebeurd, onder meer de aanstelling van een nieuwe directie. Een goed functionerende autoriteit is essentieel. In dat kader circuleren ideeën over mogelijke aanpassingen aan de wetgeving, bijvoorbeeld rond de hoogte van boetes in vergelijking met andere

réaliser au préalable une analyse d'impact sur les droits fondamentaux, en accordant une attention particulière aux groupes vulnérables? Une innovation qui suscite la méfiance n'est pas un progrès. Il ne peut y avoir d'innovation sans confiance.

La protection des enfants en ligne demeure une priorité. L'attention portée par la ministre au CSAM, au DSA et à la vérification de l'âge est justifiée, mais l'équilibre est extrêmement délicat dans cette matière. Comment la ministre évitera-t-elle que la vérification de l'âge entraîne une collecte supplémentaire de données ou une surveillance indirecte? La Belgique misera-t-elle explicitement sur des solutions respectueuses de la vie privée, telles que des modèles de vérification anonymes ou locaux?

La ministre reconnaît à juste titre que la police et les services de renseignement ont besoin de moyens modernes, mais c'est précisément là que le contrôle démocratique est crucial. Comment la ministre garantira-t-elle que les applications de l'IA utilisées dans les enquêtes n'entraînent pas de la discrimination ou du profilage? Le Parlement sera-t-il systématiquement informé des nouvelles applications dans des contextes expérimentaux?

M. Steven Matheï (cd&v) fait observer que la note de politique générale souligne clairement l'importance du thème de la vie privée, qui se reflète également dans divers débats de société. La note s'articule autour d'un cadre national et international, et annonce d'emblée une évaluation. Parallèlement, il convient de rechercher en permanence l'équilibre classique entre, d'une part, la vie privée et la protection des données à caractère personnel et, d'autre part, le développement d'initiatives susceptibles de mettre ces données sous pression.

L'intervenant se félicite de l'évaluation annoncée. Les règles du RGPD et la législation belge en matière de protection de la vie privée datent de 2018, mais les choses ont évolué rapidement depuis lors. Il est donc nécessaire de faire le point sur cette législation.

En ce qui concerne la réglementation internationale, l'intervenant s'enquiert de l'état des lieux, notamment concernant le règlement omnibus numérique et sa transposition dans la législation fédérale.

Des questions se posent également au niveau national. L'APD, qui reste un acteur important dans le domaine de la protection de la vie privée, a connu de nombreuses évolutions l'année dernière, notamment la désignation d'une nouvelle direction. Il est essentiel que cette autorité fonctionne correctement. Dans ce contexte, des idées circulent concernant d'éventuelles modifications de la

landen of het invoeren van externe leden in plaats van externe experts, zoals door de GBA zelf gesuggereerd. De spreker vraagt hoe de minister tegenover deze pistes staat.

De beleidsnota verwijst naar een enquête van 2021 als uitgangspunt voor de evaluatie. De spreker merkt op dat er de afgelopen maanden al overlegmomenten zijn geweest om zaken af te toetsen. Hij vraagt met welke organisaties dat gebeurde, wat de planning is voor de evaluatie en of alles bespreekbaar is, dan wel of men zich uitsluitend richt op de resultaten van de enquête.

Daarnaast wijst hij op het belang van rechtszekerheid: de privacyregelgeving moet persoonsgegevens beschermen, maar organisaties die gegevens verwerken moeten ook zekerheid hebben dat zij dat correct doen. De GBA werkt aan initiatieven zoals een certificeringsmodel dat grote consultancykantoren toelaat certificaten uit te reiken. Dat bevordert rechtszekerheid, maar dreigt enkel toegankelijk te zijn voor organisaties met voldoende financiële middelen. Hoe kijkt de minister naar het risico op een kloof tussen grote en kleine organisaties?

Vervolgens bespreekt het lid de samenwerking met collega-ministers. Privacy raakt aan vele beleidsdomeinen, en overleg is noodzakelijk. Dat blijkt ook uit de nota, bijvoorbeeld wat betreft de *sandboxes* die samen met de minister van Economie en de FOD Economie worden uitgewerkt. Welke concrete voorbeelden staan daarbij voor ogen?

In de beleidsnota staat ook dat wordt onderzocht of er regelluwe zones specifiek voor GDPR kunnen komen. Hoe ziet de minister dat? Bestaan er al ideeën of aanvragen en wat is de timing?

De nota verwijst voorts naar het gebruik van AI in politieel onderzoek en bij inlichtingendiensten, waar voldoende regels noodzakelijk zijn. Hoe zit het in andere beleidsdomeinen waar AI wordt gebruikt? Bestaat er een overzicht, hoe wordt dat opgevolgd en waar ligt de coördinatie? Men herinnert zich eerdere discussies over gegevens die door databrokers worden verwerkt, onder meer over medewerkers van Defensie of politie en cipiers die via apps traceerbaar zijn. De minister gaf eerder aan dat de GBA werd gevraagd om bewustmakingsacties

législation, par exemple en ce qui concerne le montant des amendes par rapport à d'autres pays ou la substitution de membres externes aux experts externes, comme l'a suggéré l'APD elle-même. L'intervenant s'enquiert de la position de la ministre à cet égard.

La note évoque, comme point de départ de l'évaluation, une enquête réalisée en 2021. L'intervenant fait observer que des concertations ont déjà été organisées ces derniers mois afin d'examiner certaines questions. Il demande avec quelles organisations ces concertations ont eu lieu, quel est le calendrier prévu pour l'évaluation et si toutes les sujets peuvent être abordés ou si l'on se concentre exclusivement sur les résultats de l'enquête.

L'intervenant souligne par ailleurs l'importance de la sécurité juridique: la réglementation en matière de protection de la vie privée doit protéger les données à caractère personnel, mais les organisations qui traitent ces données doivent également avoir la certitude qu'elles le font correctement. L'APD travaille sur des initiatives telles qu'un modèle de certification permettant aux grands cabinets de consultance de délivrer des certificats. Ces certificats favoriseront la sécurité juridique, mais risquent de n'être accessibles qu'aux organisations disposant de moyens financiers suffisants. Comment la ministre évalue-t-elle le risque de voir un fossé se creuser entre les grandes et les petites organisations?

Le membre aborde ensuite la coopération entre la ministre et ses collègues. La protection de la vie privée touchant de nombreux domaines politiques, la concertation est indispensable. La note cite notamment les zones faiblement réglementées, qui seront développées en coopération avec le ministre de l'Économie et le SPF Économie. Quels exemples concrets peut-on donner à cet égard?

La note indique également qu'une étude est en cours afin de déterminer si des zones faiblement réglementées spécifiques au RGPD peuvent être créées. Quelle est la position de la ministre à cet égard? Des idées ou des demandes ont-elles déjà été formulées et quel est le calendrier prévu?

La note précise par ailleurs que des règles suffisantes sont nécessaires pour encadrer l'utilisation de l'IA dans les enquêtes policières et par les services de renseignement. Qu'en est-il dans d'autres domaines politiques où l'IA est utilisée? Existe-t-il un aperçu, comment cette question est-elle suivie et qui est chargé de la coordination? On se souvient des discussions précédentes concernant les données traitées par les courtiers en données, concernant notamment des collaborateurs de la Défense ou de la police et des gardiens de prison, qui

op te zetten voor federale medewerkers. Hoe wordt dat gecoördineerd en hoe ziet het vervolgtraject eruit?

Het EU-US *Data Privacy Framework* (DPF) was vorig jaar een belangrijk onderwerp, waarbij werd aangegeven dat de geopolitieke context het kader mogelijk onder druk kan zetten. Een jaar later zijn er nieuwe ontwikkelingen. De spreker vraagt naar de stand van zaken en naar het Belgische standpunt in de Europese discussies.

Tot slot de leeftijdscontrole op sociale media. In de commissie voor Justitie vonden uitgebreide hoorzittingen plaats en zullen nog hoorzittingen volgen. De nota verwijst naar deze werkzaamheden en waardeert die. De spreker herhaalt dat zijn fractie voorstander is van een leeftijdsgrens, maar heeft bijkomende vragen. De GDPR voorziet vandaag al in een grens van dertien jaar. Hoe evalueert de minister de huidige handhaving van deze regel?

De spreker besluit dat de evaluatie van de privacywetgeving bijzonder belangrijk is. Hij kijkt naar de samenwerking met de commissie. Die evaluatie wordt een belangrijk ijkpunt voor de verdere bescherming van privacyregels en voor de bewustmaking van iedereen die met persoonsgegevens op een correcte manier moet omgaan.

De heer Stefaan Van Hecke (Ecolo-Groen) stelt dat privacy belangrijk is. Het is een essentieel grondrecht. In die zin is de inleiding van de beleidsnota wat verontrustend, want die start met de beschouwing dat data in de digitale wereld een essentiële, strategische grondstof is, en dat het beheersen van het gebruik ervan nieuwe kansen biedt en talrijke voordelen met zich meebrengt in verschillende sectoren van de samenleving op het gebied van innovatie, optimalisatie, efficiëntie en transparantie.

Grondrechten zijn geen grondstof. De beleidsnota van de minister en dus ook de plannen voor 2026 zijn op dat vlak behoorlijk verontrustend. De minister verklaart weliswaar te streven naar een noodzakelijk evenwicht tussen de verschillende rechten en belangen, maar wat de visie van de minister op privacy nu is en welke concrete maatregelen de minister zal nemen om de privacy van Belgische burgers te garanderen, blijft onduidelijk. De beleidsnota staat vol evaluaties, overwegingen, zaken die gevolgd en opgevolgd zullen worden, soms zelfs aandachtig. De minister herkent de spanningen tussen privacy, digitalisering, kunstmatige intelligentie en

sont traçables grâce à des applications. La ministre a précédemment indiqué que l'APD avait été chargée de mettre en place des actions de sensibilisation à l'intention des collaborateurs fédéraux. Comment cette question est-elle coordonnée et quelle sera la suite du processus?

Le cadre de protection des données UE – États-Unis (*Data Privacy Framework* – DPF) a été un sujet important l'année dernière. Il a déjà été indiqué que le contexte géopolitique pourrait compromettre ce cadre. Un an plus tard, de nouveaux développements sont intervenus. L'intervenant s'enquiert de l'état d'avancement du projet et de la position belge dans les discussions européennes.

Le dernier point abordé par l'intervenant concerne le contrôle de l'âge sur les réseaux sociaux. La commission de la Justice a organisé des auditions approfondies, et d'autres suivront. La note à l'examen souligne l'utilité de ces travaux. L'intervenant répète que son groupe est favorable à une limite d'âge, mais il a des questions complémentaires. Le RGPD prévoit déjà une limite de treize ans. Comment la ministre évalue-t-elle le contrôle actuel du respect de cette règle?

L'intervenant conclut en soulignant l'importance de l'évaluation de la législation sur la protection de la vie privée. Il évoque la coopération avec la commission. Cette évaluation constituera un point de référence important pour la protection future des règles en matière de protection de la vie privée et pour la sensibilisation de toutes les personnes qui doivent traiter correctement des données à caractère personnel.

M. Stefaan Van Hecke (Ecolo-Groen) souligne l'importance de la protection de la vie privée, qui constitue un droit fondamental essentiel. À cet égard, l'introduction de la note de politique est plutôt préoccupante, car elle commence par considérer les données du monde numérique comme une ressource clé et stratégique, dont la maîtrise offrirait de nouvelles opportunités et de nombreux avantages dans différents secteurs de la société notamment pour l'innovation, l'optimisation, l'efficacité et la transparence.

Les droits fondamentaux ne se négocient pas. La note de politique générale de la ministre, et par extension les projets pour 2026, sont particulièrement inquiétants sur ce point. Certes, la ministre affirme chercher un équilibre nécessaire entre les différents droits et intérêts, mais sa vision de la protection de la vie privée et les mesures concrètes qu'elle entend prendre pour garantir la vie privée des citoyens belges demeurent floues. La note de politique regorge d'évaluations, de considérations, d'éléments qui seront suivis et contrôlés, parfois même attentivement. La ministre reconnaît les tensions existant entre la vie privée, la numérisation, l'intelligence

veiligheid, maar verbindt daar vervolgens geen enkele politieke consequentie aan.

Hoe zal België intern en binnen Europa een rol spelen? Zal België een voortrekkersrol of beschermingsambitie opnemen? De beleidsnota van de minister is uitgesproken procedureel en evaluatief, maar vermijdt keuzes, prioriteiten en concrete doelstellingen.

Van de minister mag men toch meer verwachten. De spreker zegt behoorlijk ontgoocheld te zijn.

Hij wil beginnen met de ontwikkelingen van het laatste jaar, die de laatste maanden nog grotere urgentie hebben gekregen, met name de omgang van de Verenigde Staten en Amerikaanse techbedrijven met de data en privacy van burgers. Het is duidelijk dat noch de huidige Amerikaanse regering, noch de grote techbedrijven die close zijn met president Trump, ook maar iets geven om de privacy van onze burgers. Daarom de volgende vragen.

Hoeveel data die de Belgische overheid bezit van haar burgers worden eigenlijk aangehouden op Amerikaanse servers? Welke garanties heeft de minister dat data, die de Belgische overheid bezit van haar burgers en die op servers van Amerikaanse bedrijven worden bijgehouden op Europees grondgebied, niet naar de VS getransfereerd worden? En hoe garandeert de minister dat deze data niet door deze techbedrijven of de Amerikaanse overheid opgeslagen en eventueel gebruikt kunnen worden? Wat is het plan van aanpak van de minister daarover? Wat is haar standpunt?

In de beleidsnota verwijst de minister ook naar het EU-US *Data Privacy Framework*, waar ze schrijft dat de ontwikkelingen met betrekking tot dat framework tot doel hebben de overdracht van gegevens tussen de Europese Unie en de Verenigde Staten te vergemakkelijken. Die zullen ook met bijzondere aandacht worden gevolgd door de administratie van de minister, wordt gezegd. Maar over welke ontwikkelingen heeft de minister het en wat bedoelt ze met "bijzondere aandacht"?

Wat is de visie van de minister rond de problemen met dit framework? Jarenlang bleef de vraag of het opslaan van persoonsgegevens in Amerikaanse clouddiensten in overeenstemming is met de Europese privacywetgeving een juridisch en politiek mijnenveld. Hoewel de Europese Unie en de VS herhaaldelijk hebben geprobeerd kaders vast te stellen om trans-Atlantische gegevensstromen mogelijk te maken, hebben deze overeenkomsten consequent geen stand gehouden bij de juridische toetsing.

artificielle et la sécurité, mais n'en tire ensuite aucune conséquence politique.

Quel rôle la Belgique entend-elle jouer au niveau national et européen? Adoptera-t-elle une attitude pionnière ou plutôt protectrice? La note de la ministre reste très procédurale et évaluative, mais elle ne précise ni choix, ni priorités, ni objectifs concrets.

On est pourtant en droit d'attendre davantage de la part de la ministre. L'intervenant se dit profondément déçu.

Il souhaite commencer par les développements de l'an passé, dont l'urgence s'est encore accrue ces derniers mois, notamment pour ce qui est du traitement des données et de la vie privée des citoyens par les États-Unis et les entreprises technologiques américaines. Il est clair que ni l'actuel gouvernement américain, ni les grandes entreprises technologiques proches du président Trump ne se soucient de la vie privée de nos citoyens, d'où les questions suivantes.

Combien de données que l'État belge détient sur ses citoyens sont en réalité hébergées sur des serveurs américains? Quelles garanties la ministre possède-t-elle pour que les données détenues par l'État belge, même lorsqu'elles sont stockées sur des serveurs d'entreprises américaines en Europe, ne soient pas transférées aux États-Unis? Comment s'assure-t-elle que ces données ne puissent être stockées et éventuellement utilisées par ces entreprises technologiques ou par l'administration américaine? Quel est le plan d'action de la ministre à ce sujet? Quelle est sa position?

Dans la note de politique, la ministre fait également référence à l'*EU-US Data Privacy Framework*, en indiquant que les évolutions concernant ce cadre visent à faciliter le transfert de données entre l'Union européenne et les États-Unis. Il est précisé que ces évolutions seront suivies avec une attention particulière par l'administration de la ministre. Mais de quelles évolutions la ministre parle-t-elle exactement et qu'entend-t-elle par "attention particulière"?

Quelle est la vision de la ministre concernant les problèmes liés à ce cadre? Pendant des années, la question de savoir si le stockage de données personnelles dans des services cloud américains était conforme à la législation européenne sur la protection de la vie privée a constitué un véritable champ de mines juridique et politique. Bien que l'Union européenne et les États-Unis aient tenté à plusieurs reprises de mettre en place des cadres permettant les flux de données transatlantiques, ces accords n'ont jamais résisté à l'épreuve juridique.

Vanuit juridisch oogpunt zijn de uitspraken van het Hof van Justitie van de Europese Unie over trans-Atlantische gegevensoverdrachten duidelijk. Tenzij de VS ingrijpende juridische hervormingen doorvoeren, biedt geen enkel kader voldoende bescherming volgens de EU-wetgeving. De algemene verordening gegevensbescherming vereist dat persoonsgegevens worden beschermd met een beveiligingsniveau dat gelijkwaardig is aan dat binnen de EU.

Volgens de Amerikaanse wetgeving hebben buitenlandse burgers echter niet dezelfde privacyrechten als inwoners van de VS. De Amerikaanse inlichtingendiensten hebben ruime toegang tot gegevens die zijn opgeslagen door in de VS gevestigde bedrijven. Dat betekent dat organisaties die persoonsgegevens uit de EU verwerken moeten beoordelen of doorgiften aan in de VS gevestigde cloudproviders in overeenstemming zijn met de AVG. In de praktijk is dat moeilijk, zo niet onmogelijk, zonder aanvullende waarborgen zoals versleuteling, gegevenslokalisatie of alternatieve hostingoplossingen.

Wat is de visie van de minister daarop? Kunnen bedrijven en andere organisaties ervan uitgaan dat wanneer ze het DPF volgen, ze wettelijk in orde zijn? Of riskeren ze in de problemen te komen? Gelooft de minister dat de regering-Trump respect heeft voor de bescherming van de privacy van Europese burgers, ook al holt zij alle toezichtsorganen volledig uit? Welke maatregelen zal de minister nemen of op Europees niveau voorstellen om te voorkomen dat de gegevens van Belgische burgers in handen vallen of blijven van Amerikaanse inlichtingendiensten?

Wat betreft het onderdeel digitale soevereiniteit zijn organisaties in Europa, ook overheden, ondertussen erg afhankelijk van de Amerikaanse cloud. Ook heel wat bedrijven zijn naar de cloud van Microsoft, Amazon of Google gemigreerd. En nu is men dus ook de AI van onder meer Microsoft aan het omarmen. Zo maak je jezelf alweer extra afhankelijk. De cloud vormt een enorm risico op het vlak van privacy, want de Amerikaanse regering kan er toegang toe eisen via diverse wetten.

En zoals een deskundige ook zei, zou je eigenlijk belangrijke organisaties, zeker diegene die actief zijn rond vitale infrastructuur of met veel data van burgers omgaan, moeten verplichten om de continuïteit van hun digitale systemen te waarborgen. Ze moeten bijvoorbeeld kunnen aantonen dat als Microsoft, Amazon of Google uitvalt, om welke reden dan ook, ze aan medicijndistributie kunnen blijven doen. Men moet kunnen garanderen dat ziekenhuizen nog bij hun patiëntengegevens kunnen om mensen te blijven verzorgen en op te volgen.

D'un point de vue juridique, les décisions de la Cour de justice de l'Union européenne sur les transferts de données transatlantiques sont claires. Sauf si les États-Unis entreprennent des réformes juridiques majeures, aucun cadre ne garantit une protection suffisante au regard de la législation européenne. Le Règlement général sur la protection des données (RGPD) exige que les données personnelles soient protégées à un niveau équivalent à celui appliqué au sein de l'UE.

Cependant, selon la législation américaine, les citoyens étrangers ne disposent pas des mêmes droits à la vie privée que les résidents des États-Unis. Les services de renseignement américains ont un large accès aux données stockées par des entreprises établies aux États-Unis. Ainsi, les organisations traitant des données personnelles en provenance de l'UE doivent évaluer si les transferts vers des fournisseurs de cloud américains sont conformes au RGPD. Dans la pratique, cela s'avère difficile, voire impossible, sans garanties supplémentaires telles que le chiffrement, la localisation des données ou des solutions d'hébergement alternatives.

Quelle est la position de la ministre à ce sujet? Les entreprises et autres organisations peuvent-elles considérer que le suivi du DPF garantit leur conformité légale? Ou, risquent-elles d'avoir des problèmes? La ministre estime-t-elle que l'administration Trump respecte la protection de la vie privée des citoyens européens, alors même qu'elle affaiblit tous les organes de contrôle? Quelles mesures la ministre compte-t-elle prendre, ou proposer au niveau européen, pour éviter que les données des citoyens belges ne tombent entre les mains des services de renseignement américains?

Concernant la souveraineté numérique, les organisations en Europe, y compris les autorités publiques, dépendent fortement du cloud américain. De nombreuses entreprises ont migré vers les clouds de Microsoft, Amazon ou Google. Elles adoptent désormais aussi l'IA proposée par ces mêmes acteurs, ce qui renforce encore leur dépendance. Le cloud représente donc un risque majeur pour la vie privée, le gouvernement américain pouvant en exiger l'accès en vertu de différentes lois.

Comme l'a aussi souligné un expert, il faudrait en réalité obliger les grandes organisations, notamment celles liées aux infrastructures critiques ou traitant de nombreuses données personnelles, à assurer la continuité de leurs systèmes numériques. Elles doivent par exemple pouvoir démontrer que, si Microsoft, Amazon ou Google tombaient en panne, elles pourraient malgré tout continuer à distribuer des médicaments. Il faut également pouvoir garantir l'accès des hôpitaux aux dossiers de leurs patients afin de poursuivre les soins et le suivi.

Maar de beleidsnota zwijgt over afhankelijkheid van Amerikaanse cloud- en AI-infrastructuur en het verband met privacy. Dus zijn de vragen: hoe verhoudt het privacybeleid van de minister zich tot digitale soevereiniteit? Welke maatregelen zal de minister hier ondernemen? Zal de minister bijvoorbeeld werk maken van een toegenomen gebruik van opensourcesoftware, zodat de gegevens van België niet in handen zijn van buitenlandse techbedrijven en bovendien gemakkelijk kunnen worden overgezet wanneer bepaalde buitenlandse technologie om welke reden dan ook niet langer toegankelijk is?

En dat leidt tot een aantal nauw gerelateerde Europese ontwikkelingen. De minister beschrijft die zelfs zonder een standpunt in te nemen, terwijl de minister als bevoegd minister de Belgische visie hieromtrent natuurlijk moet uitdragen binnen de Raad en de diensten van de minister het Belgische standpunt in de voorbereidende vergaderingen eveneens moeten uitdragen.

Wat betreft de AVG herkent de minister het belang ervan. Tegelijkertijd lijkt ze enigszins positief te staan tegenover de digitale omnibus die de Europese Commissie heeft voorgesteld. Dat houdt nochtans in dat de AVG en de AI Act sterk worden afgezwakt.

Digitaliseringsexpert Passchier waarschuwde in *De Standaard* nog dat als dat doorgaat – en die kans is best groot – er dertig jaar wordt teruggedaan in de tijd. Er is dan ook verbazing en bezorgdheid dat met dit voorstel de AVG opnieuw wordt herzien en in de kern wordt afgezwakt, onder meer inzake de definitie van persoonsgegevens. De mogelijke wijzigingen die meer flexibiliteit voor AI-training mogelijk maken, zijn bijzonder verontrustend, omdat ze de deur kunnen openen voor het gebruik van persoonsgegevens en gevoelige gegevens zonder voldoende waarborgen.

Grondrechten moeten zwaarder wegen dan financiële belangen. Hetzelfde geldt voor elke poging om de huidige regels over cookies en de integriteit van terminals, die gebaseerd zijn op de toestemming van de gebruiker, af te zwakken.

Wat is de houding van de minister en de regering over de verschillende privacyafzwakkingen in de digitale omnibus? Welk standpunt heeft de minister daarover de voorbije maanden ingenomen en welk standpunt zal ze de komende maanden innemen? Er wordt graag een duiding verkregen over wat nu eigenlijk het Belgische standpunt is en zal zijn, en hoe de minister *chat control* evalueert, want er zijn nog vergaderingen gepland de komende maanden, op onder meer 26 februari, 4 mei en in juni. Er staat nog heel wat op het spel. Hoe verhoudt de minister zich tot het verlengen van de huidige verordening die communicatiedienstverleners zoals

Toutefois, la note ne traite pas de la dépendance aux infrastructures cloud et d'IA américaines, ni de son lien avec la protection de la vie privée. Les questions sont donc: comment la politique de confidentialité de la ministre s'articule-t-elle avec la souveraineté numérique? Quelles mesures prévoit-elle? Envisage-t-elle, par exemple, de favoriser un recours accru aux logiciels open source, afin que les données belges restent protégées et puissent être facilement transférées si certaines technologies étrangères deviennent, pour quelle que raison que ce soit, indisponibles?

Ces questions s'inscrivent dans plusieurs développements européens étroitement liés. Mme Verlinden en décrit même les éléments sans prendre de position, alors qu'en tant que ministre compétente, elle devrait naturellement faire valoir la vision belge à ce sujet au sein du Conseil, et ses services devraient également défendre la position belge lors des réunions préparatoires.

La ministre reconnaît l'importance du RGPD. Dans le même temps, elle semble plutôt favorable à l'omnibus numérique proposé par la Commission européenne. Cela implique néanmoins un affaiblissement considérable du RGPD et de l'AI Act.

L'expert en numérisation Passchier avertissait encore dans *De Standaard* que, si cette évolution se poursuit – ce qui est assez probable –, on ferait un pas en arrière de trente ans. Il est donc inquiétant que cette proposition conduise à une révision et à un affaiblissement du RGPD, notamment sur la définition des données à caractère personnel. Les changements possibles, qui offriraient plus de flexibilité pour l'entraînement de l'IA, sont particulièrement préoccupants, car ils pourraient permettre l'utilisation de données personnelles et sensibles sans garanties suffisantes.

Les droits fondamentaux doivent primer sur les intérêts financiers. Il en va de même pour toute tentative visant à affaiblir les règles actuelles relatives aux cookies et à l'intégrité des terminaux, qui reposent sur le consentement de l'utilisateur.

Quel est le point de vue de la ministre et du gouvernement sur les assouplissements relatifs à la vie privée contenus dans l'omnibus numérique? Quelle position la ministre a-t-elle adoptée ces derniers mois, et qu'en sera-t-il dans les mois à venir? Il serait, en effet, utile d'obtenir des précisions sur la position belge actuelle et future, ainsi que sur l'évaluation par la ministre du *chat control*, d'autant que d'autres réunions sont prévues dans les prochains mois, notamment les 26 février, 4 mai et en juin. L'enjeu est encore de taille. Que pense la ministre du prolongement du règlement actuel, qui permet aux fournisseurs de services de communication – Facebook,

Facebook, Messenger, Gmail of Instagram toestaat om af te wijken van de bestaande wetgeving inzake gegevensbescherming?

Tot slot heeft de minister bij de bespreking van de plannen voor 2025 tal van beloften en intenties uitgesproken voor het eigen beleid. Welke concrete resultaten heeft de aangekondigde evaluatie van de privacywet sinds 2025 opgeleverd? Welke bepalingen van titel 2 en 7 worden prioritair herzien en met welke doelstelling?

Er wordt ook meer duiding gevraagd rond de GBA. In de vorige beleidsnota erkende de minister de wettelijke verplichting om voldoende middelen ter beschikking te stellen, want er is inderdaad een nood aan grotere financiering. In deze beleidsnota wordt er niets meer vermeld over de middelen, de werklust en de handhavingscapaciteit. De vraag rijst waarom in 2026 geen maatregelen worden aangekondigd om de structurele onderbezetting van de GBA aan te pakken.

En hoe verhoudt de ambitie om AI-data en experimenteerzones te faciliteren zich tot een toezichthouder die nu al overbevraagd is? Er zijn ook vragen over de verhoudingen tussen de GBA en de VTC. De minister had aangekondigd om daar een samenwerkingsakkoord over te sluiten of in overleg te gaan. Wat is er sinds vorig jaar gebeurd?

De minister had vorige keer ook aandacht besteed aan wetenschappelijk onderzoek en gerechtelijke dossiers en de uitdagingen die zich daar stellen. In de nota staat dat overleg met het College van procureurs-generaal bevestigd is. Het doel blijft vaag: identificeren wat moet wijzigen. Welke concrete acties zullen volgen en welke concrete wetswijzigingen worden overwogen?

B. Antwoorden van de minister

De minister beantwoordt de vragen als volgt:

— Beschermingsniveau

De hoorzittingen hebben de gelegenheid geboden om dieper in te gaan op het gewenste beschermingsniveau, een beleidskeuze die een combinatie van maatregelen vergt. Er zijn verschillende benaderingen mogelijk en de maatregelen moeten complementair zijn. Het door de commissie besproken voorstel van resolutie (DOC 56 1039/001) focust op twee aspecten: gecontroleerde pseudonimiteit en leeftijdscontrole, waarvoor de deskundigen de voorwaarden hebben vastgesteld die moeten waarborgen dat het recht op privacy en de fundamentele vrijheden daadwerkelijk worden geëerbiedigd.

Messenger, Gmail ou Instagram – de déroger à la législation sur la protection des données?

Pour conclure, lors de la discussion des plans pour 2025, la ministre a formulé de nombreuses promesses et intentions concernant sa propre politique. Quels résultats concrets l'évaluation annoncée de la législation sur la protection de la vie privée a-t-elle produits depuis 2025? Quelles dispositions des titres 2 et 7 sont révisées en priorité et dans quel objectif?

Des éclaircissements sont également demandés concernant l'APD. Dans la note précédente, la ministre reconnaissait l'obligation légale de prévoir des moyens suffisants et la nécessité d'un financement accru. La note de cette année, en revanche, ne fait plus aucune mention des moyens, de la charge de travail, ni de la capacité d'exécution. La question se pose donc de savoir pourquoi aucune mesure n'est annoncée pour 2026 afin de remédier au sous-effectif structurel de l'Autorité.

Comment concilier l'ambition de faciliter l'accès aux données de l'IA et la création de zones d'expérimentation avec un régulateur déjà très sollicité? Des questions demeurent aussi quant aux relations entre l'APD et la VTC. La ministre avait annoncé un accord de coopération ou l'ouverture de concertations à ce sujet. Quelles avancées ont eu lieu depuis l'an dernier?

Enfin, la ministre avait précédemment attiré l'attention sur la recherche scientifique et les dossiers judiciaires, ainsi que sur les défis associés. La note confirme la concertation avec le Collège des procureurs généraux, mais l'objectif reste flou: identifier les ajustements nécessaires. Quelles actions concrètes en résulteront et quelles modifications législatives sont envisagées?

B. Réponses de la ministre

La ministre répond aux questions comme suit.

— Niveau de protection

Les auditions ont permis d'approfondir la question du niveau de protection souhaité, un choix politique nécessitant une combinaison de mesures. Plusieurs approches sont possibles et il doit y avoir une complémentarité entre les actions. La proposition de résolution (DOC 56 1039/001) examinée par la commission met l'accent sur deux axes: le pseudonymat vérifié et la vérification de l'âge, pour lesquels les experts ont identifié les conditions garantissant efficacité et respect du droit à la vie privée et des libertés fondamentales.

De leeftijdscontrole past in het kader van de Europese DSA, in het bijzonder artikel 28, en van de Europese *Digital Wallet*. De Europese Commissie bevestigt dat de lidstaten die controle verplicht kunnen maken bij het gebruik van sociale media. Het is niet de bedoeling het beleid te fragmenteren, maar wel om voordeel te halen uit het Europese kader voor digitale identiteit teneinde de minderjarigen in België beter te beschermen.

De bezorgdheid over de privacy werd weggenomen, met name via een studie van het Europees Comité voor gegevensbescherming waarin leeftijdsverificatie werd aangemerkt als de minst ingrijpende methode om de leeftijd te controleren. Er bestaan technische oplossingen om de leeftijdscontrole uit te breiden naar minderjarigen onder de zestien, onder andere via de applicatie *itsme*, die met die functionaliteit zal worden uitgebreid.

Gecontroleerde pseudonimiteit kan worden geïmplementeerd zonder risico op massacontrole noch aantasting van de vrijheid van meningsuiting. Dat aspect wordt nader toegelicht in de beleidsnota over digitale technologie.

— Identificatie van plegers van onlinegeweld

Deze identificatie is hachelijk en vol hindernissen. De sleutels daartoe zijn vaak in handen van de platforms zelf. Het recht en de persoonlijke levenssfeer zouden beter worden beschermd, mocht de overheid de nodige hefboomen in handen hebben voor gerechtelijke procedures tegen de plegers van onlinegeweld.

— Tijdlijn

Op Belgisch niveau zijn de wetgevende werkzaamheden gelijktijdig met het werk in de commissie aangevat. Ze zullen de komende maanden worden voortgezet, met als doel nog dit jaar een tekst aan de regering voor te leggen. Het tijdpad zal worden beïnvloed door het werk van de leden van de commissie voor Justitie: hun aanbevelingen zullen worden opgenomen zodra ze beschikbaar zijn, bij voorkeur in de komende weken.

Het klopt dat er in Frankrijk snel vooruitgang wordt geboekt.

Die vergelijking moet echter genuanceerd worden: het is makkelijker snel vooruitgang te boeken zonder de technische procedures te ontwikkelen die nodig zijn om de principes waarover men het eens is geworden, effectief te implementeren.

Meerdere landen hebben leeftijdsbeperkingen ingevoerd, maar vaak met fragiele controlesystemen.

La vérification de l'âge s'inscrit dans le cadre européen du DSA, spécialement de son article 28, et du *Digital Wallet* européen. La Commission européenne confirme que les États membres peuvent imposer cette vérification sur les réseaux sociaux. Il ne s'agit pas de fragmentation, mais de mettre à profit le cadre européen en matière d'identité digitale pour protéger davantage les mineurs en Belgique.

Les inquiétudes liées à la vie privée ont trouvé des réponses, notamment via une étude du Comité européen de la protection des données qui identifie la vérification de l'âge comme la méthode d'assurance d'âge la moins intrusive. Les solutions techniques existent pour étendre la vérification d'âge aux mineurs de moins de 16 ans, y compris via *itsme*, qui travaille à cette fonctionnalité.

Le pseudonymat vérifié peut être mis en œuvre sans risque de contrôle de masse ni atteinte à la liberté d'expression. Ce volet est davantage développé dans la note consacrée au numérique.

— Identification des auteurs de violences en ligne

Cette identification est hasardeuse et semée d'obstacles. Ceux qui en détiennent souvent les clés sont les plateformes elles-mêmes. Le droit et la vie privée serait mieux protégé si les pouvoirs publics disposaient des capacités nécessaires dans le cadre de procédures judiciaires menées contre les auteurs de violences en ligne.

— Ligne du temps

Au niveau belge, un travail de préparation législative a été entamé parallèlement aux travaux menés en commission. Ce travail se poursuivra dans les prochains mois, avec l'objectif de soumettre un texte au gouvernement encore cette année. Le calendrier sera influencé par le travail des membres de la commission de la Justice: leurs recommandations seront intégrées dès qu'elles seront disponibles, de préférence dans les prochaines semaines.

Concernant la France, il est exact que les avancées y sont rapides.

Il convient toutefois de nuancer cette comparaison: il est plus aisé de progresser rapidement lorsqu'on ne développe pas les modalités techniques nécessaires à la mise en œuvre effective des principes adoptés.

Plusieurs États ont instauré des limitations d'âge, mais souvent avec des systèmes de vérification fragiles.

Het doel is niet vooruitgang te boeken om een symbolisch resultaat te bereiken, maar ervoor te zorgen dat de regels effectief worden toegepast.

De regelingen die thans in andere landen worden toegepast, zijn echter niet alleen weinig betrouwbaar, maar ook problematisch: ze laten het aan de platforms zelf over om de leeftijd van de gebruikers te beoordelen, waardoor die gevoelige gegevens over jongeren, hun voorkeuren en hun gewoonten in handen krijgen.

Wetgeving die de leeftijd voor toegang tot sociale media beperkt, moet daarom worden ondersteund door een robuust controlesysteem.

Het voorbeeld van identiteitscontroles bij de ingang van nachtclubs is een goede illustratie van de aanpak die wordt nagestreefd: een eenvoudige, betrouwbare controle op basis van een officieel document. De exacte leeftijd zal worden bepaald op basis van de aanbevelingen van de commissie, maar eenmaal de beslissing genomen moet de controle volledig en effectief zijn.

Tegenwoordig is de registratie van jongeren op de sociale media gebaseerd op niet-geverifieerde leeftijdsverklaringen, waardoor de regel onwerkzaam is.

Dat controle- of authenticatiesysteem kan ook worden gebruikt om regels op te stellen met betrekking tot online-anonimiteit. In dit stadium worden geen persoonlijke gegevens doorgegeven via applicaties zoals itsme. Het is een interface om de identiteit van een gebruiker te bevestigen bij een federale overheid, zonder gegevens te extraheren. Het systeem controleert gewoon of de persoon die een handeling uitvoert, daadwerkelijk is wie hij beweert te zijn.

Bonvendien kan de digitale portefeuille een oplossing voor leeftijdsverificatie bevatten.

— Bevoegdheden van de deelstaten

Het is belangrijk transversaal actie te ondernemen, maar het is duidelijk dat elk bestuursniveau zijn eigen bevoegdheden heeft. De preventieve en educatieve aspecten vallen onder de bevoegdheid van de gemeenschappen en het is de moeite waard de geboekte vooruitgang te benadrukken, in het bijzonder het actieplan dat voor Kerstmis 2025 in Vlaanderen werd voorgesteld, alsook de regeringsbeslissing die in juli 2025 door de Franse Gemeenschap werd aangenomen.

De problematiek van de bescherming van minderjarigen en het deel van de inspanning dat elke bevoegde minister moet leveren, worden vaak besproken bij het bepalen van het Belgische standpunt op Europees niveau.

L'objectif n'est pas d'avancer pour afficher un résultat symbolique, mais de garantir l'effectivité des règles.

Or, les dispositifs actuellement utilisés dans d'autres pays sont non seulement peu fiables, mais également problématiques: ils laissent aux plateformes la responsabilité d'évaluer elles-mêmes l'âge des utilisateurs, ce qui conduit à la collecte de données sensibles sur les jeunes, leurs préférences et leurs usages.

Une législation limitant l'âge d'accès aux réseaux sociaux doit donc impérativement s'appuyer sur un système robuste de vérification.

L'exemple du contrôle d'identité à l'entrée d'une boîte de nuit illustre bien l'approche recherchée: une vérification simple, fiable et fondée sur un document officiel. La question de l'âge exact relève des recommandations de la commission, mais une fois la décision prise, la vérification doit être complète et effective.

Aujourd'hui, l'inscription des jeunes sur les réseaux sociaux repose sur des déclarations d'âge non vérifiées, ce qui rend la règle inopérante.

Ce système de vérification ou d'authentification peut également servir pour encadrer l'anonymat en ligne. À ce stade, aucun transfert de données personnelles n'est opéré via des applications comme itsme. Il s'agit d'une interface permettant de confirmer l'identité d'un utilisateur auprès d'une autorité fédérale, sans extraction de données. Le système vérifie simplement que la personne qui effectue une démarche est bien celle qu'elle prétend être.

Par ailleurs, le portefeuille digital pourra intégrer une solution de vérification de l'âge.

— Compétences des entités fédérées

Il importe de mener une action transversale, mais il est clair que chaque niveau de pouvoir dispose de ses propres compétences. Le volet préventif et éducatif relève des communautés, et il convient de souligner les avancées réalisées, notamment le plan d'action présenté en Flandre avant Noël 2026 ainsi que la décision gouvernementale adoptée par la Fédération Wallonie-Bruxelles en juillet 2025.

La question de la protection des mineurs et la part de l'effort que chaque ministre compétent doit fournir font régulièrement l'objet de discussions lors de la définition de la position belge au niveau européen.

Op basis van de rapporten, contacten en gevoerde hoorzittingen lijkt het noodzakelijk voortgang te boeken.

— Alomvattend samenwerkingsakkoord met de deelstaten

Met betrekking tot het samenwerkingsakkoord met de deelstaten wordt gesteld dat het akkoord een praktisch instrument zal zijn. Het moet de uitwisseling tussen de administraties en verenigingen omkaderen met het respect van de bevoegdheden van elke entiteit. Er worden gesprekken opgestart met de deelstaatcollega's om eerst de noden, mogelijkheden, de scope en de methode te bepalen vooraleer technische stappen worden gezet.

Het akkoord zal de rechtspraak van het Grondwettelijk Hof strikt respecteren. Elke verwerking van persoonsgegevens moet gebaseerd zijn op een formele wet. De wet bepaalt het doel, welke gegevens worden verwerkt, wie de ontvangers zijn, hoelang de gegevens worden bewaard en welke garanties er zijn voor de betrokken burgers. Een samenwerkingsakkoord kan deze wettelijke basis nooit vervangen. Het doel is enkel om de administratieve samenwerking te verbeteren met garanties voor gegevensverwerking en de preventie van datalekken, incidenten en cyberaanvallen.

— Digitale soevereiniteit

Dit aspect wordt nader toegelicht in de beleidsnota over digitale technologie.

Het is positief dat sommige mondiale leveranciers steeds meer rekening houden met de Europese bezorgdheden inzake soevereiniteit. Europa staat niet machteloos tegenover Amerikaanse bedrijven die buiten het raamwerk opereren.

Op de Amerikaanse cloud is thans het *Privacy Framework* van toepassing, dat garandeert dat de bedrijven die zich daarbij aansluiten een beschermingsniveau bieden dat gelijkwaardig is aan de AVG. Dit betekent echter niet dat deze oplossingen ideaal zijn of dat we geen alternatieven moeten ontwikkelen. Daarom wordt op Europees niveau gewerkt aan de *Cloud & AI Development Act*.

Tegelijk wordt een Belgische cloud- en datacenterstrategie opgezet, gebaseerd op een duidelijk principe: de oplossingen afstemmen op het niveau van gegevensencryptie, volgens een aanpak die meerdere opties combineert.

Sur la base des rapports, des échanges et des auditions menées, il apparaît nécessaire d'avancer.

— Accord de coopération global avec les entités fédérées

En ce qui concerne l'accord de coopération avec les entités fédérées, il est précisé que cet accord constituera un instrument pratique. Il devra encadrer les échanges entre les administrations et les associations, dans le respect des compétences de chaque entité. Des discussions seront engagées avec les collègues des entités fédérées afin de déterminer d'abord les besoins, les possibilités, le champ d'application et la méthode, avant d'entamer des étapes techniques.

L'accord respectera strictement la jurisprudence de la Cour constitutionnelle. Tout traitement de données à caractère personnel doit reposer sur une loi formelle. La loi doit déterminer la finalité, les données traitées, les destinataires, la durée de conservation des données ainsi que les garanties offertes aux citoyens concernés. Un accord de coopération ne peut jamais remplacer cette base légale. L'objectif est uniquement d'améliorer la coopération administrative, avec des garanties en matière de traitement des données et de prévention des fuites de données, des incidents et des cyberattaques.

— Souveraineté numérique

Ce volet est davantage développé dans la note de politique générale consacrée à la politique numérique.

Il est positif que certains fournisseurs mondiaux intègrent de plus en plus les préoccupations européennes en matière de souveraineté. L'Europe n'est pas impuissante par rapport aux entreprises américaines qui opèrent en dehors du cadre.

Le cloud américain est désormais régi par le *Privacy Framework*, qui garantit que les entreprises qui y adhèrent offrent un niveau de protection équivalent à celui du RGPD. Cela ne signifie toutefois pas que ces solutions soient idéales ou qu'elles ne doivent pas nous inciter à développer des alternatives. C'est pourquoi des travaux sont menés au niveau européen sur le *Cloud & AI Development Act*.

En parallèle, une stratégie belge en matière de cloud et de data centers est en cours de mise en place, fondée sur un principe clair: adapter les solutions au niveau de l'encryption des données, dans une approche combinant plusieurs options.

— Evaluatie en ontwikkeling

Het doel is de privacywet aan te passen. Meer specifiek moet titel 7 over het COC worden aangepast om volledig in overeenstemming te zijn met de Europese wetgeving en de recente rechtspraak. Het huidige systeem van onrechtstreekse toegang via het COC leidt er soms toe dat burgers een formeel antwoord ontvangen zonder voldoende informatie over de uitgevoerde controle. Die situatie schenkt geen voldoening. De rechtspraak van het Hof van Justitie van de Europese Unie en van het hof van beroep te Brussel vereist aanpassingen. Het COC moet meer informatie kunnen geven aan de betrokkenen en zij moeten echt de mogelijkheid hebben in beroep te gaan. De rechter moet ook over alle nodige informatie beschikken om een juiste beslissing te kunnen nemen. Er wordt technisch werk verricht en er worden wetgevende initiatieven genomen. Het Europese raamwerk moet volledig worden toegepast, teneinde de rechten van de burgers te versterken en een effectieve controle te garanderen, met inachtneming van het noodzakelijke evenwicht met de openbare veiligheid.

Wat de evaluatie van de privacywet betreft, bekijkt de administratie alle vragen en voorstellen uit de praktijk naar aanleiding van de eerste evaluatie. Daarbij wordt nagegaan of ze nog relevant zijn.

Op basis daarvan wordt een tweede evaluatie voorbereid met een duidelijke methode en duidelijke doelstellingen. Dit werk is al gestart. De teams van de minister hebben opnieuw contact opgenomen met verschillende actoren op het terrein.

Het doel is dit jaar te beschikken over een sterk en goed onderbouwd beeld van de situatie, zodat een concreet actueel en doeltreffend wetsontwerp kan worden uitgewerkt.

De werkzaamheden op Europees niveau om de toepassing van het raamwerk voor gegevensbescherming te vereenvoudigen, met name voor de bedrijven, worden nauwlettend gevolgd. De Commissie heeft het voorstel voor een digitale omnibusverordening gepresenteerd. Het beoogt de administratieve rompslomp te verminderen en de digitale regels samenhangender te maken. Het moet ook de relatie tussen de AVG en de AI Act verduidelijken.

Deze tekst bevat gerichte verbeteringen. Hij definieert met name het begrip wetenschappelijk onderzoek en verduidelijkt de status van gepseudonimiseerde gegevens, wanneer die niet kunnen worden geheridentificeerd door de verwerkingsverantwoordelijke. Hij vereenvoudigt ook bepaalde verplichtingen, bijvoorbeeld inzake het enige aanspreekpunt voor datastromen.

— Évaluation et évolution

L'objectif est d'adapter la loi sur la vie privée, plus spécifiquement, le titre 7 relatif au COC, doit être adapté pour assurer une pleine conformité avec le droit européen et la jurisprudence récente. Le système actuel d'accès indirect via le COC conduit parfois les citoyens à recevoir une réponse formelle sans information suffisante sur le contrôle effectué. Cette situation n'est pas satisfaisante. La jurisprudence de la Cour de Justice de l'Union européenne et de la cour d'appel de Bruxelles impose des ajustements. Le COC doit pouvoir fournir davantage d'informations aux personnes concernées, et celles-ci doivent disposer d'une véritable possibilité de recours. Le juge doit également disposer de toutes les informations nécessaires pour statuer correctement. Un travail technique est en cours et des initiatives législatives sont prises. Le cadre européen doit être pleinement appliqué, afin de renforcer les droits des citoyens et de garantir un contrôle effectif, tout en respectant l'équilibre nécessaire avec la sécurité publique.

En ce qui concerne l'évaluation de la loi vie privée, l'administration examine l'ensemble des questions et propositions issues de la pratique à la suite de la première évaluation et vérifie si elles sont toujours pertinentes.

Sur cette base, une deuxième évaluation est en cours de préparation, selon une méthode et des objectifs clairement définis. Ce travail a déjà débuté. Les équipes de la ministre ont repris contact avec différents acteurs de terrain.

L'objectif est de disposer cette année d'une vision solide et étayée de la situation, afin d'élaborer un projet de loi concret, actualisé et efficace.

Les travaux menés au niveau européen visant à simplifier l'application du cadre de la protection des données, notamment pour les entreprises, sont suivis de près. La Commission a présenté le projet de règlement *Digital Omnibus*, dont l'objectif est d'alléger la charge administrative et de renforcer la cohérence des règles numériques. Il vise également à clarifier l'articulation entre le RGPD et l'AI Act.

Ce texte apporte des avancées ciblées. Il précise notamment la notion de recherche scientifique et clarifie le statut des données pseudonymisées, lorsqu'elles ne peuvent pas être réidentifiées par le responsable du traitement. Il simplifie aussi certaines obligations, par exemple en ce qui concerne le point de contact unique pour les flux de données.

Het Belgische standpunt over dat voorstel zal worden bepaald in samenspraak met de federale partners en de deelstaten. Er zijn echter belangrijke voorbehouden gemaakt: innovatie en vereenvoudiging worden gesteund indien relevant, maar het blijft essentieel een hoog niveau van bescherming van de grondrechten te behouden. De AVG en de AI Act moeten sterke referenties blijven en dat standpunt werd ook verdedigd.

— *Digital Omnibus*

De *Digital Omnibus* heeft als doel het Europese digitale raamwerk te harmoniseren en te vereenvoudigen en aldus het concurrentievermogen van de Europese Unie in een mondiale context te verbeteren.

Waakzaamheid blijft geboden ten aanzien van het stimuleren van de competitiviteit van de economie enerzijds en de bescherming van grondrechten anderzijds, en dan in het bijzonder het recht op privacy.

Sommige vereenvoudigingsmaatregelen zijn nuttig, andere kunnen gevolgen hebben voor de bescherming van persoonsgegevens. Het is van cruciaal belang dat de Europese garantiebasis niet wordt verzwakt.

De lidstaten hebben hun vragen aan de Europese Commissie doorgegeven. Op basis hiervan zal België de voorstellen analyseren en in overleg met de federale regering en de deelstaten de nodige aanpassingen bepalen om ervoor te zorgen dat economische doorstellingen de fundamentele rechten niet in gevaar brengen.

De Europese Unie mag niet dereguleren ten koste van de grondrechten. Het debat rond de *Digital Omnibus* toont trouwens aan dat de standpunten uiteenlopen. Hoewel de Commissie beweert zich te baseren op de rechtspraak van het Hof van Justitie van de Europese Unie, is het ontbreken van een voorafgaande effectbeoordeling betreurenswaardig. Een dergelijke analyse is essentieel om te garanderen dat de grondrechten geenszins worden geschonden.

Er werd advies gevraagd aan het Europees Comité voor gegevensbescherming, dat een beslissende rol zal spelen bij het innemen van een standpunt. Er is steun voor een vereenvoudiging ter ondersteuning van de bedrijven maar niet in ruil voor deregulering. Over de grondrechten kunnen geen compromissen worden gesloten en dat evenwicht wordt verdedigd in de Europese besprekingen.

La position belge sur cette proposition sera définie en concertation avec les partenaires fédéraux et les entités fédérées. Des réserves importantes ont toutefois été émises: si l'innovation et la simplification sont soutenues lorsqu'elles sont pertinentes, la préservation d'un haut niveau de protection des droits fondamentaux demeure essentielle. Le RGPD et l'AI Act doivent rester des références fortes, et cette position a été défendue.

— *Digital Omnibus*

Le *Digital Omnibus* vise à harmoniser et à simplifier le cadre numérique européen, renforçant ainsi la compétitivité de l'Union européenne dans un contexte mondial.

La vigilance reste de mise entre, d'une part, la stimulation de la compétitivité économique et, d'autre part, la protection des droits fondamentaux, et en particulier du droit à la vie privée.

Certaines mesures de simplification sont utiles, mais d'autres peuvent impacter la protection des données personnelles. Il est crucial que le socle de garantie européen ne soit pas fragilisé.

Les États membres ont transmis leurs questions à la Commission européenne. Sur cette base, la Belgique analysera les propositions et, en concertation avec le gouvernement fédéral et les entités fédérées, déterminera les adaptations nécessaires afin de garantir que les objectifs économiques ne mettent pas en péril les droits fondamentaux.

L'Union européenne ne peut pas déréguler au détriment des droits fondamentaux. Le débat autour du *Digital Omnibus* montre d'ailleurs que les positions sont partagées. Bien que la Commission affirme s'appuyer sur la jurisprudence de la Cour de Justice de l'Union européenne, l'absence d'une analyse d'impact préalable est regrettable. Une telle analyse est indispensable pour garantir qu'aucune atteinte ne soit portée aux droits fondamentaux.

Un avis du Comité européen de la protection des données a été demandé et jouera un rôle déterminant dans la prise de position. La simplification destinée à soutenir les entreprises est soutenue, mais pas au prix d'une dérégulation. Aucun compromis n'est possible sur les droits fondamentaux, et cet équilibre est défendu dans les discussions européennes.

— Organieke wet van de Gegevensbeschermingsautoriteit

De wet van 25 december 2023 heeft al enkele aanpassingen aan de organieke wet aangebracht, maar dit werk is niet afgerond.

Het Grondwettelijk Hof heeft duidelijk gesteld dat essentiële regels zoals de ontvankelijkheid van klachten en de bemiddeling in de wet zelf moeten worden vastgelegd en niet in een intern reglement. Het Hof heeft hiervoor een deadline opgelegd: 31 december 2026.

Het respecteren van deze termijn is een absolute prioriteit. Het doel is de werking van de GBA juridisch te versterken en te zorgen voor volledige grondwettelijke conformiteit van het wettelijk kader.

De hervorming gebeurt in overleg met de GBA en de gelegenheid wordt aangegrepen om andere verbeteringen te onderzoeken indien dat nodig blijkt.

— Only Once

Deze kwestie valt onder de bevoegdheid van de vice-eersteminister en minister van Begroting, belast met Administratieve Vereenvoudiging. In samenspraak met hem werd een wetgevingsinitiatief genomen.

Het doel van de minister in die context is de formaliteiten te beperken, de efficiëntie te verhogen en een gemoderniseerde administratie te ondersteunen. Voor het overige wordt verwezen naar de vice-eersteminister.

— Veiligheid van gegevens

Gegevensbeveiliging is een topprioriteit. Het voorkomen van lekken, incidenten en cyberaanvallen is cruciaal voor de overheid.

Het Centrum voor Cybersecurity België coördineert de nationale strategie, ook voor de overheidsdiensten. In geval van een lek geldt de wettelijke verplichting om het CCB en de Gegevensbeschermingsautoriteit op de hoogte te brengen.

Algemene cyberveiligheid valt onder de bevoegdheid van de minister van Binnenlandse Zaken, maar voor de federale administratie valt dit onder de bevoegdheid van de minister die het woord heeft en die erop zal erop toezien dat de regels van veiligheid en gegevensbescherming strikt worden nageleefd.

Wat het gebruik van gegevens voor wetenschappelijke doeleinden betreft, ligt de toegang tot gegevens in gerechtelijke dossiers moeilijk omdat de regels streng

— Loi organique de l'Autorité de protection des données

La loi du 25 décembre 2023 a déjà apporté certaines modifications à la loi organique, mais ce travail n'est pas achevé.

La Cour constitutionnelle a clairement indiqué que des règles essentielles, telles que la recevabilité des plaintes et la médiation, doivent être inscrites dans la loi elle-même et non dans un règlement interne. Elle a fixé une échéance à cet effet: le 31 décembre 2026.

Le respect de ce délai constitue une priorité absolue. L'objectif est de renforcer juridiquement le fonctionnement de l'APD et d'assurer la pleine conformité constitutionnelle du cadre légal.

La réforme est menée en concertation avec l'APD et l'occasion est saisie pour examiner d'autres améliorations si cela s'avère nécessaire.

— Only Once

Il s'agit d'une question qui relève de la compétence du vice-premier ministre et ministre du Budget, chargé de la Simplification administrative. En concertation avec ce dernier, une initiative législative a été prise.

L'objectif de la ministre dans ce cadre consiste à limiter les formalités et augmenter l'efficacité et soutenir une administration modernisée. Pour le reste, il est renvoyé au vice premier ministre.

— Sécurité des données

La sécurité des données est une priorité absolue. La prévention des fuites, incidents et cyberattaques est cruciale pour les pouvoirs publics.

Le Centre pour la Cybersécurité belge coordonne la stratégie nationale, y compris pour les administrations. En cas de fuite, la loi impose une notification au CCB et à l'Autorité de protection des données.

La cybersécurité générale relève de la compétence du ministre de l'Intérieur mais, pour l'administration fédérale, elle relève de la compétence de la ministre, qui veillera au strict respect des règles de sécurité et de protection des données.

Quant à l'usage des données à des fins scientifiques, l'accès aux données – contenues dans les dossiers judiciaires – est difficile, les règles étant sévères.

zijn. Anonimisering is duur en magistraten moeten toestemming geven om dossiers te gebruiken. Er moet een evenwicht zijn tussen privacy, het geheim van het onderzoek en het wetenschappelijke onderzoek. In de praktijk is dat evenwicht moeilijk te vinden en dat vertraagt het onderzoek.

Er is een werkgroep opgericht met de vertegenwoordigers van de hoven en rechtbanken, het openbaar ministerie en het Hof van Cassatie. Die groep analyseert de situatie en werkt aan een voorstel voor een wetswijziging en procedures om veilige toegang tot gerechtelijke dossiers te vergemakkelijken.

De zaak zal nauwlettend worden opgevolgd in het kader van de *Digital Omnibus*, met als doel rigoureuze wetenschappelijk onderzoek te waarborgen en tegelijk de grondrechten van de burgers te beschermen.

— EU-US Data Privacy Framework

De trans-Atlantische situatie is gespannen, maar het *Framework* blijft geldig en functioneert. Het Europese Hof heeft het Franse beroep afgewezen en de Amerikaanse presidentiële decreten zijn nog steeds van kracht. De gegevensstromen worden dus niet verstoord.

Elke beslissing die de bestaande garanties zou kunnen bedreigen wordt met een waakzaam oog gevolgd. De Europese Commissie houdt de situatie nauwgezet in de gaten. Bedrijven wordt aangeraden eveneens gebruik te maken van standaardcontracten en clausules of *binding corporate rules*.

De prioriteiten van België zijn duidelijk: rechtsonzekerheid vermijden en samenwerken met de Commissie bij problemen. Men moet ervoor zorgen dat privacy en persoonsgegevens daadwerkelijk bij trans-Atlantische gegevensstromen worden beschermd.

— CSAM

Beelden van kindermisbruik zijn een plaag, met al maar jongere slachtoffers. Het regeerakkoord maakt van de bestrijding van die vorm van criminaliteit een prioriteit.

De genomen maatregelen op digitaal gebied en voor de bescherming van de privacy hebben tot doel de veiligheid van de systemen te waarborgen en tegelijk kinderen online te beschermen. De beginselen van noodzakelijkheid en evenredigheid vormen het referentiekader.

De CSAM-verordening werd binnen de regering besproken en er werd een akkoord over bereikt in de

L'anonymisation est coûteuse et les magistrats doivent autoriser l'utilisation des dossiers. Il convient de trouver un équilibre entre le respect de la vie privée, le secret de l'instruction et la recherche scientifique. En pratique, cet équilibre est difficile à atteindre, ce qui ralentit la recherche.

Un groupe de travail a été constitué avec des représentants des cours et tribunaux, du ministère public et de la Cour de cassation. Ce groupe analyse la situation et élabore une proposition de modification législative ainsi que des procédures visant à faciliter un accès sécurisé aux dossiers judiciaires.

Il y aura un suivi attentif en lien avec le *Digital Omnibus* pour garantir une recherche scientifique rigoureuse tout en protégeant les droits fondamentaux des citoyens.

— EU-US Data Privacy Framework

La situation transatlantique est tendue, mais le *Framework* demeure valable et fonctionne. La Cour européenne a rejeté le recours français et les décrets présidentiels américains sont toujours en vigueur. Les flux de données ne sont donc pas perturbés.

Toute décision susceptible de menacer les garanties existantes est suivie avec vigilance. La Commission européenne surveille étroitement la situation. Il est également recommandé aux entreprises de recourir à des contrats et à des clauses types ou à des règles d'entreprise contraignantes (*binding corporate rules*).

Les priorités de la Belgique sont claires: éviter l'insécurité juridique et coopérer avec la Commission en cas de difficultés. Il convient de veiller à ce que la vie privée et les données à caractère personnel soient effectivement protégées dans le cadre des flux transatlantiques de données.

— CSAM

La pédopornographie est un fléau qui touche des victimes de plus en plus jeunes. L'accord de gouvernement fait une priorité de la lutte contre cette forme de criminalité.

L'action menée en matière de numérique et de protection de la vie privée vise à garantir la sécurité des systèmes tout en protégeant les enfants en ligne. Les principes de nécessité et de proportionnalité constituent le cadre de référence.

Le règlement CSAM a été discuté au sein du gouvernement et a fait l'objet d'un accord au Conseil européen,

Europese Raad, opdat de politiediensten en het gerecht de broodnodige onderzoeken kunnen voeren. In het trialoogoverleg wordt momenteel gekeken naar de verankering van het systeem voor vrijwillige detectie. Het CSAM-dossier wordt met bijzondere aandacht gevolgd, teneinde de minderjarigen te beschermen en tegelijk de fundamentele vrijheden te respecteren.

Het is evenwel betreurenswaardig dat de trialoogbesprekingen vooral focussen op de oprichting van het Europees centrum en op meer consensuele vragen, ten koste van een grondig debat over het evenwicht tussen de bescherming van minderjarigen en de eerbiediging van de persoonlijke levenssfeer, dat nog steeds ontoereikend is. Dat gebrek aan inhoudelijk debat is zorgwekkend.

Het dossier verdient een ambitieuzere en evenwichtiger aanpak.

— Sandboxes

Een zogeheten *regulatory sandbox* is een gecontroleerde omgeving voor het testen van technologieën of systemen voor artificiële intelligentie. In een dergelijke omgeving kunnen innovaties onder reële omstandigheden worden ontwikkeld en gevalideerd, voor een beperkte periode en onder supervisie van de toezichthoudende autoriteit.

Het doel is tweeledig. Bedrijven ruimte bieden om te innoveren en om te verzekeren dat de innovaties van bij het begin voldoen aan de wettelijke regels, vooral op het vlak van privacy. Het is geen wetteloos gebied maar een begeleid en gecontroleerd experiment.

De oprichting van *sandboxes* is opgenomen in het regeerakkoord. De Europese *AI Act* vereist dat de oprichting voor augustus 2026 gebeurt en de AVG staat dit soort systemen toe.

Een onderzoek werd vorig jaar afgerond. De FOD Economie bereidt nu een wetontwerp voor om een passend juridische kader voor bedrijven te creëren.

Om een regelgevend kader te creëren voor die regelruwe experimenteerzones zullen de eventueel nodige bijstellingen worden voorgesteld van de wet tot oprichting van de Gegevensbeschermingsautoriteit.

Elke technologie wordt getest in een strikt gecontroleerde omgeving onder toezicht van de bevoegde autoriteiten, zonder de privacy van personen in gevaar te brengen.

afin de permettre aux services de police et de justice de mener les enquêtes indispensables. Le Trilogue examine actuellement la pérennisation du mécanisme de détection volontaire. Le suivi de ce dossier s'effectue avec une attention particulière, dans l'objectif de protéger les mineurs tout en respectant les libertés fondamentales.

Il est toutefois regrettable que les discussions en Trilogue se concentrent principalement sur la création du centre européen et les questions plus consensuelles, au détriment d'un débat approfondi sur l'équilibre entre la protection des mineurs et le respect de la vie privée, qui reste insuffisant. Cette absence de réflexion de fond est préoccupante.

Ce dossier mérite une approche plus ambitieuse et plus équilibrée.

— Bacs à sable

Un bac à sable réglementaire est un environnement contrôlé pour tester des technologies ou des systèmes d'intelligence artificielle. Il permet de développer et valider des innovations en conditions réelles pour une durée limitée et sous la supervision de l'autorité de contrôle.

L'objectif est double. Offrir aux entreprises un espace pour innover et veiller à ce que les innovations soient conformes dès le départ aux règles légales, en particulier en matière de respect de la vie privée. Il ne s'agit pas d'une zone de non-droit mais d'une expérimentation encadrée et contrôlée.

L'accord du gouvernement le prévoit. L'*AI Act* européen impose leur création avant août 2026 et le RGPD autorise ce type de dispositif.

Une enquête a été finalisée l'année dernière. Le SPF Économie prépare à présent un projet de loi en vue de créer un cadre juridique adéquat pour les entreprises.

Les ajustements à la loi portant création de l'Autorité de protection des données seront, si nécessaire, proposées afin de créer un cadre réglementaire pour ces zones d'expérimentation faiblement réglementées.

Chaque technologie est testée dans un environnement strictement contrôlé, sous la supervision des autorités compétentes, sans mettre en danger la vie privée des personnes.

— Conventie 108+ van de Raad van Europa

Voor de ratificatie van Conventie 108+ moet eerst titel 3 van de wet op de bescherming van de persoonlijke levenssfeer, die de inlichtingendiensten en het OCAD regelt, worden aangepast, met name wat de toegang van particulieren tot hun gegevens betreft. De komende maanden zullen de betrokken actoren worden geraadpleegd. Op basis daarvan kunnen wetsvoorstellen worden opgesteld alvorens België tot ratificatie van de conventie overgaat.

Voor het tijdspad wordt een ruime marge genomen: ongeveer een jaar voor de onderhandelingen, een jaar voor de wetwijzigingen en een jaar voor de aanneming van de instemmingswet. Het doel is de ratificatie van de conventie binnen ongeveer drie jaar rond te hebben.

— Privacy als mensenrecht

De beleidsnota en de beleidsinitiatieven houden absoluut rekening met de artikelen 7 en 8 van het Handvest van de Grondrechten van de Europese Unie, artikel 16 van het EU-verdrag en artikel 8 van het Europees Verdrag voor de Rechten van de Mens.

Die rechten moeten worden afgewogen tegen andere grondrechten, zoals de vrijheid van meningsuiting en van informatie, het recht op vrijheid en veiligheid, het recht op werk en het recht op een eerlijk proces. De AVG herinnert er ook aan dat gegevensbescherming moet worden verzoend met de vrijheid van meningsuiting, de volksgezondheid, de bestuurlijke transparantie en de vrijheid van wetenschappelijk onderzoek. Met dat in gedachten is het vinden van een evenwicht tussen die verschillende rechten cruciaal.

De rechtspraak van de internationale instellingen wordt volledig in acht genomen.

— VTC

Er wordt de voorkeur gegeven aan een aanpak die gebaseerd is op overleg en het algemeen belang. In 2025 heeft een ontmoeting plaatsgevonden met de nieuwe directie van de GBA, waarbij dit dossier werd besproken.

Een gezamenlijke werkwijze zal binnenkort worden vastgelegd en vervolgens worden meegedeeld. Daarbij wordt gestreefd naar een efficiënte samenwerking, met respect voor zowel de bevoegdheden van de GBA als die van de VTC.

— Convention 108+ du Conseil de l'Europe

La ratification de la Convention 108+ nécessite au préalable une adaptation du titre 3 de la loi sur la vie privée, qui encadre les services de renseignement et l'OCAM, notamment en ce qui concerne l'accès des particuliers à leurs données. Une consultation des acteurs concernés est prévue dans les prochains mois. Sur cette base, des propositions législatives pourront être élaborées avant que la Belgique ne puisse procéder à la ratification de la convention.

En termes de calendrier, une large marge est envisagée: environ un an de négociations, un an pour la modification des textes législatifs et un an pour l'adoption de la loi d'assentiment. L'objectif est d'aboutir à la ratification de cette convention dans un délai d'environ trois ans.

— Le respect de la vie privée, un droit fondamental

La note de politique générale et les initiatives politiques tiennent pleinement compte des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, de l'article 16 du Traité sur l'Union européenne et de l'article 8 de la Convention européenne des droits de l'homme.

Ces droits doivent être mis en balance avec d'autres droits fondamentaux, tels que la liberté d'expression et d'information, le droit à la liberté et à la sûreté, le droit au travail ou encore le droit à un procès équitable. Le RGPD rappelle également que la protection des données doit être conciliée avec la liberté d'expression, la santé publique, la transparence administrative ou la liberté de la recherche scientifique. Dans cette perspective, la recherche d'un équilibre entre ces différents droits demeure essentielle.

La jurisprudence des juridictions internationales est pleinement respectée.

— Vlaamse Toezichtcommissie (VTC)

La ministre privilégie une approche fondée sur la concertation et l'intérêt général. En 2025, une rencontre a eu lieu avec la nouvelle direction de l'APD, au cours de laquelle ce dossier a été examiné.

Une méthode de travail commune sera prochainement arrêtée puis communiquée. L'objectif est d'assurer une coopération efficace, dans le respect tant des compétences de l'APD que de celles de la VTC.

De VTC heeft echter beroep aangetekend tegen een beslissing van de GBA. Dat heeft onvermijdelijk een reeks juridische en procedurele gevolgen, wat de voortgang van de werkzaamheden enigszins vertraagt. De minister geeft geen verdere commentaar bij de situatie. Ze stelt vast dat de wet beroep mogelijk maakt en dat het de betrokken partijen toekomt hun rechten uit te oefenen via de wettelijke kanalen, voor het Marktenhof. Wat het samenwerkingsakkoord tussen de GBA en de VTC betreft, blijven overleg en het nastreven van het algemeen belang de prioriteit.

— Filosofisch-politieke beschouwingen

De beleidsnota is niet het resultaat van beschouwingen over de werking van de markt. Ze probeert een scheidslijn te trekken tussen de economische belangen en de bescherming van de grondrechten. Er moet ruimte zijn voor innovatie, maar met inachtneming van de persoonlijke levenssfeer. De beleidsnota verwijst naar tal van initiatieven om dat evenwicht te waarborgen, met bescherming van de persoonsgegevens.

Het kan niet worden ontkend dat het grootschalige gebruik van persoonsgegevens, zeker in een alomtegenwoordige digitale omgeving, risico's voor de burgers meebrengt. Zelfs de strengste regelgeving biedt burgers vandaag geen volledige controle over hun gegevens.

Het optreden van de minister toont aan wat voor haar de zorgpunten zijn en hoe ze het evenwicht beoogt te herstellen. De meest kwetsbare mensen in de samenleving verdienen des te meer een toereikende mate van bescherming.

C. Replieken van de leden

De heer Khalil Aouasti (PS) vernam graag meer over de alomvattende visie van de minister. Misschien moet de organisatie van de parlementaire werkzaamheden worden herzien. Inhoudelijk werden meerdere belangrijke standpunten opnieuw bevestigd: geen compromissen op het stuk van de grondrechten, de noodzaak om elke vorm van Europese deregulering te voorkomen, het belang van voorafgaande impactanalyses – nog altijd op Europees niveau – en de voorkeur voor een robuust openbaar systeem voor leeftijdsverificatie. Die elementen vormen de essentiële klijtlijnen, die niet altijd duidelijk naar voren kwamen in de beleidsnota maar wel werden verduidelijkt tijdens de parlementaire bespreking.

Digitale soevereiniteit blijft bovenaan op de agenda staan. De Europese en Belgische bezorgdheden omtrent de *cloud* en datacenters vereisen een eigen strategie,

Un recours a cependant été introduit par la VTC contre une décision de l'APD. Cette démarche entraîne inévitablement une série de conséquences juridiques et procédurales, ce qui ralentit quelque peu l'avancement des travaux. La ministre ne commente pas davantage la situation. Elle constate que le recours est prévu par la loi et il revient aux parties concernées d'exercer leurs droits par les voies légales, devant la Cour des marchés. S'agissant de l'accord de coopération entre l'APD et la VTC, la priorité reste la concertation et la poursuite de l'intérêt général.

— Remarques de philosophie politique

La note de politique générale n'est pas le résultat de considérations relatives au fonctionnement du marché. Elle essaye de tracer une ligne de démarcation bien au milieu entre les intérêts économiques d'une part, et la protection des droits fondamentaux de l'autre. Il y a lieu de permettre l'innovation, tout en respectant la vie privée des personnes. La note renvoie à de nombreuses initiatives visant à garantir l'équilibre en question, avec une protection accordée aux données à caractère privé.

On ne peut nier que l'utilisation à grande échelle de données à caractère personnel, en particulier dans un environnement numérique omniprésent, comporte des risques pour les citoyens. Même la réglementation la plus stricte ne garantit aujourd'hui pas aux citoyens un contrôle total sur leurs données.

L'action de la ministre illustre ses préoccupations et démontrent sa volonté de rétablir un équilibre. Les membres les plus fragiles de la société méritent d'autant plus un degré de protection suffisant.

C. Répliques des membres

M. Khalil Aouasti (PS) apprécierait de pouvoir connaître la vision globale de la ministre. Peut-être convient-il de repenser l'organisation des travaux parlementaires. Quant au fond, un ensemble de positions importantes a été réaffirmé: l'absence de compromis sur les droits fondamentaux, la nécessité d'éviter toute dérégulation européenne, l'importance d'analyses d'impact préalables – toujours au niveau européen – et la préférence pour un système public et robuste de vérification de l'âge. Ces éléments constituent des balises essentielles du débat, qui n'apparaissaient pas toujours clairement dans la note de politique générale mais qui ont été précisés au cours des échanges parlementaires.

Les discussions sur la souveraineté numérique demeurent centrales. Les préoccupations européennes et belges en matière de *cloud* et de data centers exigent

met name gezien de risico's die samenhangen met het Amerikaanse wettelijk raamwerk, zoals de *Patriot Act* – oorspronkelijk een instrument voor terrorismebestrijding, maar inmiddels vooral gebruikt voor industriële spionage – waardoor Amerikaanse bedrijven toegang mogen krijgen tot gegevens die in Europa zijn opgeslagen. Die waakzaamheid is des te meer geboden daar de economische belangen van Europa en de Verenigde Staten niet langer systematisch samenvallen.

Inzake de ratificatie van de Conventie 108+ valt het volgens de aangekondigde termijnen te verwachten dat het proces tegen de volgende parlementsverkiezingen rond zal zijn, op voorwaarde dat de verschillende stappen zonder vertraging kunnen worden doorlopen. Met betrekking tot de CSAM-verordening is het jammer dat het Europese debat te beperkt blijft en niet alle aspecten van de bescherming van minderjarigen behelst. Een ambitieuzere benadering is wenselijk.

De leeftijdsverificatie op sociale media vereist een grondige technische analyse, inzake zowel de openbare oplossingen (digitale portefeuille *MyGov.be*, itsme) als de risico's op omzeiling. Gelijklopend daarmee reikt de *Digital Services Act* hefboomen aan om de grote platforms ertoe te verplichten inhoud aan te passen aan de leeftijd van de gebruiker, wat onder de federale bevoegdheden valt in het raam van de dialoog met die actoren.

Tot slot rest er een vraag met betrekking tot de studie van de FOD Economie over de regelluwe zones. Kan die aan de leden worden meegedeeld? Zo ja, hoe?

D. Bijkomende antwoorden van de minister

Het thema leeftijdsverificatie maakt deel uit van een breder debat over onlineanonymiteit en het evenwicht tussen de bescherming van de minderjarigen, de persoonlijke levenssfeer en de vrijheid van meningsuiting. Vooraleer de regering een wetgevend initiatief neemt, zou het nuttig zijn om in het raam van de parlementaire werkzaamheden een technische presentatie van de verschillende verificatiesystemen te geven in de commissie.

De bepaling van de toepasselijke leeftijd vormt een aparte discussie. De minister staat ter beschikking om de dialoog met het Parlement over dit en andere onderwerpen voort te zetten.

De studie over een regelgevingskader voor de zogenoemde regelluwe experimenteerzones wordt thans door meerdere kabinetten gezamenlijk onderzocht. Als die tot overeenstemming komen, kan worden overwogen dat

une stratégie propre, notamment face aux risques liés au cadre juridique américain, tel que le *Patriot Act* – qui se voulait initialement comme un instrument de lutte contre le terrorisme, mais qui entre-temps s'est développé notamment dans le cadre d'un espionnage industriel – qui peut permettre l'accès à des données stockées en Europe par des entreprises américaines. Cette vigilance est d'autant plus nécessaire que les intérêts économiques européens et américains ne coïncident plus systématiquement.

Concernant la ratification de la Convention 108+, les délais annoncés situent l'achèvement du processus à l'horizon des prochaines législatives, sous réserve que les différentes étapes puissent être atteintes sans retard. S'agissant du règlement CSAM, il est regrettable que le débat européen reste trop limité et ne couvre pas l'ensemble des enjeux de protection des mineurs. Une approche plus ambitieuse est souhaitée.

La question de la vérification de l'âge sur les réseaux sociaux nécessite une analyse technique approfondie, tant pour les solutions publiques (portefeuille e-gov, itsme) que pour les risques de contournement. Parallèlement, le *Digital Services Act* offre des leviers pour imposer aux grandes plateformes des mécanismes d'adaptation des contenus en fonction de l'âge, ce qui relève des compétences fédérales dans le cadre du dialogue avec ces acteurs.

Enfin, une demande subsiste concernant l'étude du SPF Économie sur les zones faiblement réglementées, afin de déterminer si et comment elle peut être communiquée aux membres.

D. Réponses complémentaires de la ministre

La question de la vérification de l'âge s'inscrit dans un débat plus large sur l'anonymat en ligne et l'équilibre entre la protection des mineurs, la vie privée et la liberté d'expression. Avant toute initiative législative de la part du gouvernement, il serait utile qu'une présentation technique des différents systèmes de vérification puisse être faite au sein de la commission, dans le cadre des travaux parlementaires.

La fixation de l'âge applicable relève d'une réflexion distincte. La ministre est disponible afin de poursuivre les échanges avec le Parlement sur ce sujet ou d'autres.

Enfin, s'agissant de l'étude relative aux bacs à sable réglementaires, celle-ci fait actuellement l'objet d'une analyse politique conjointe entre plusieurs cabinets. Si un accord intervient entre les équipes concernées, la

document te bezorgen. Er zij echter op gewezen dat het een werkdocument betreft. Het dient als basis voor een wetsontwerp dat thans door de FOD Economie wordt voorbereid en geeft nog geen definitief standpunt weer.

Die studie strekt ertoe een evenwichtig wetgevingskader uit te werken dat innovatie mogelijk maakt en tegelijkertijd een gereguleerde omgeving garandeert die voldoet aan de vereisten op het stuk van de grondrechten.

De rapporteur,
Christoph D'Haese

De voorzitter,
Ismaël Nuino

transmission de ce document pourra être envisagée. Il s'agit toutefois d'un document de travail servant de base à un projet de loi en préparation au SPF Économie et ne reflétant pas encore une position arrêtée.

Cette étude vise à élaborer un cadre législatif équilibré, permettant l'innovation tout en garantissant un environnement régulé et conforme aux exigences en matière de droits fondamentaux.

Le rapporteur,
Christoph D'Haese

Le président,
Ismaël Nuino