DOC 55 **2053/001**

CHAMBRE DES REPRÉSENTANTS
DE BELGIQUE

19 mai 2021

PROPOSITION DE RÉSOLUTION

relative à la gestion, à l'utilisation et au traitement des données à caractère personnel, notamment en matière de santé

(déposée par
Mme Laurence Hennuy et consorts)

BELGISCHE KAMER VAN
VOLKSVERTEGENWOORDIGERS

19 mei 2021

VOORSTEL VAN RESOLUTIE

betreffende het beheer, het gebruik en de verwerking van persoonsgegevens, met name inzake gezondheid

(ingediend door
mevrouw Laurence Hennuy c.s.)

N-VA	:	*Nieuw-Vlaamse Alliantie*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
PS	:	*Parti Socialiste*
VB	:	*Vlaams Belang*
MR	:	*Mouvement Réformateur*
CD&V	:	*Christen-Democratisch en Vlaams*
PVDA-PTB	:	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Open Vld	:	*Open Vlaamse liberalen en democraten*
Vooruit	:	*Vooruit*
cdH	:	*centre démocrate Humaniste*
DéFI	:	*Démocrate Fédéraliste Indépendant*
INDEP-ONAFH	:	*Indépendant – Onafhankelijk*

Abréviations dans la numérotation des publications:		*Afkorting bij de numering van de publicaties:*	
DOC 55 0000/000	*Document de la 55e législature, suivi du numéro de base et numéro de suivi*	*DOC 55 0000/000*	*Parlementair document van de 55e zittingsperiode + basisnummer en volgnummer*
QRVA	*Questions et Réponses écrites*	*QRVA*	*Schriftelijke Vragen en Antwoorden*
CRIV	*Version provisoire du Compte Rendu Intégral*	*CRIV*	*Voorlopige versie van het Integraal Verslag*
CRABV	*Compte Rendu Analytique*	*CRABV*	*Beknopt Verslag*
CRIV	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*	*CRIV*	*Integraal Verslag, met links het defi nitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)*
PLEN	*Séance plénaire*	*PLEN*	*Plenum*
COM	*Réunion de commission*	*COM*	*Commissievergadering*
MOT	*Motions déposées en conclusion d'interpellations (papier beige)*	*MOT*	*Moties tot besluit van interpellaties (beigekleurig papier)*

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

Le droit au respect de la vie privée constitue un droit fondamental, ferment de notre démocratie. L'avènement des technologies nous invite à questionner les relations nouvelles coexistantes entre la démocratie, l'e-gouvernance, les libertés individuelles et le recours aux solutions numériques par les organes tant publics que privés. Dans ces mouvements constants qu'engendrent le recours au numérique et l'utilisation des données à caractère personnel, la sauvegarde des droits humains doit primer. Les techniques nouvelles ne doivent jamais se développer au détriment de notre démocratie; elles ne peuvent en aucune façon la fragiliser. Il est dès lors essentiel d'adopter une position constructive quant à l'utilisation de la technologie eu égard aux normes les plus strictes en matière de protection des données à caractère personnel et de libertés individuelles.

Le contexte sanitaire actuel impose de prendre des mesures pour combattre la propagation du SARS-CoV-2, des mesures sans précédent qui font ressortir de manière flagrante l'importance du droit à la protection des données à caractère personnel. En effet, l'usage du numérique dans la maîtrise de l'épidémie est vite apparu comme une évidence. Pour répondre aux spécificités de la crise liée au COVID-19 – sa propagation rapide, son caractère invisible, sa portée asymptomatique chez certaines personnes, entre autres – les traçages à la fois manuel et automatique sont alors devenus des outils de régulation dans la stratégie adoptée: isoler, tester, tracer. Cependant, les données de santé sont les données les plus sensibles, les plus personnelles, celles qui touchent à notre vie la plus privée. Si l'on ne traite pas les données de santé avec précaution, l'on porte atteinte, non seulement à la vie privée, mais aussi aux principes d'égalité et de non-discrimination[1]. Ainsi, les données traitées dans le cadre de la lutte contre le COVID-19 sont principalement des données liées à la santé, mais pas uniquement. Il importe donc que toutes les garanties nécessaires soient prises tant légalement qu'opérationnellement pour que leur utilisation soit sécurisée et proportionnée par rapport aux objectifs poursuivis.

Les applications mobiles ont trouvé des utilisations nouvelles qui ont permis une réponse inédite dans la lutte contre le COVID-19. Le traçage a nécessité la collecte

[1] Audition de Mme Elise Degrave (Professeure à l'UNamur), 10 mars 2021, Commission de l'Intérieur, de la Sécurité, de la Migration et des Matières administratives de la Chambre.

TOELICHTING

DAMES EN HEREN,

Het recht op de eerbiediging van de privacy is een fundamenteel recht, de grondslag van onze democratie. Door de opkomst van technologieën worden wij genoopt na te gaan hoe de democratie, *e-governance*, de individuele vrijheden en het gebruik van digitale technieken door openbare én particuliere instanties voortaan kunnen samengaan. In de context van die permanente evolutie ingevolge het gebruik van digitale technologie en van persoonsgegevens moet de vrijwaring van de mensenrechten voorop staan. De ontwikkeling van nieuwe technologieën mag nooit ten koste gaan van onze democratie en mag deze op geen enkele manier ondermijnen. Het is derhalve van essentieel belang een constructieve houding aan te nemen ten aanzien van het gebruik van technologie, met inachtneming van de striktste normen inzake de bescherming van persoonsgegevens en van individuele vrijheden.

De huidige gezondheidscontext vereist ongeziene maatregelen om de verspreiding van SARS-CoV-2 tegen te gaan, waarbij overduidelijk blijkt hoe belangrijk het recht op bescherming van persoonsgegevens is. Al spoedig bleek het immers de evidentie zelve dat de epidemie zou worden aangepakt met behulp van digitale technologie. Gezien de eigenheden van de COVID-19-crisis – zoals de snelle verspreiding en de onzichtbaarheid van het virus, alsook de asymptomatische besmetting van sommige personen – zijn zowel de manuele als de automatische tracering reguleringsinstrumenten van de gevolgde strategie (afzonderen, testen, traceren) geworden. Gezondheidsgegevens zijn echter de gevoeligste en de meest persoonlijke gegevens, die betrekking hebben op het intiemste leven. Wanneer onzorgvuldig met de gezondheidsgegevens wordt omgesprongen, wordt niet alleen inbreuk gepleegd op de persoonlijke levenssfeer, maar ook op de beginselen van gelijkheid en van non-discriminatie[1]. Zo zijn de gegevens waarmee in het kader van de COVID-19-bestrijding wordt gewerkt, hoofdzakelijk (maar niet uitsluitend) gezondheidsgerelateerde gegevens. Het is dan ook belangrijk dat zowel wettelijk als operationeel alle nodige waarborgen worden ingebouwd, om ervoor te zorgen dat het gebruik ervan beveiligd verloopt en in verhouding staat tot de nagestreefde doelstellingen.

De mobiele toepassingen hebben nieuwe gebruiksvormen ingang doen vinden die een ongeziene respons in de strijd tegen COVID-19 hebben bewerkstelligd. Voor

[1] Hoorzitting met mevrouw Elise Degrave (hoogleraar aan de UNamur), 10 maart 2021, in de Kamercommissie voor Binnenlandse Zaken, Veiligheid, Migratie en Bestuurszaken.

de données personnelles (contacts de personnes, GSMs/e-mails, lieux fréquentés, …) qui ont dû être couplées avec des données disponibles dans les bases de données de l'État (santé ou ONSS, par exemple). Les bases de données relatives à la vaccination, aux symptômes de la maladie, supposent le recueil, le traitement, le stockage ou la communication de données à caractère personnel de santé. Par exemple, la Banque Carrefour de la Sécurité Sociale (BCSS) centralise de nombreuses données liées au COVID-19 (données de contacts, d'identification, de travail, de résidence) des travailleurs salariés et indépendants. La télémédecine qui s'est développée sous l'effet de la pandémie a aussi généré une utilisation nouvelle de telles données.

Ces initiatives de recueil et de "couplage" de données rendent le problème encore plus sensible. Bien qu'elles visent toutes des objectifs sanitaires d'intérêt général, il convient que le Règlement *général sur la protection des données* (*RGPD*) soit respecté et que la finalité du traitement des données à caractère personnel et le principe de proportionnalité soient définis avec précision. Le caractère adéquat, pertinent et non excessif du traitement au regard des finalités poursuivies doit rester la clef de voûte du système. Les balises incontournables garantissant la protection de la vie privée doivent être démocratiquement définies, débattues et acceptées. Tout écart par rapport à ces balises réduira la protection de la vie privée et des données à caractère personnel. En effet, les techniques de couplage de données (*data matching*) et d'exploration de données (*data mining*) réalisées grâce à des algorithmes peuvent mener à des profilages et dérives graves[2]. En ce sens, pour que le citoyen puisse faire confiance à l'État dans sa gestion des bases de données, les questions de gouvernance et de traitement des données doivent être appréhendées de manière exemplaire.

En Belgique, nous fonctionnons en recourant à un modèle de gestion des données décentralisé, les données étant stockées dans différentes bases de données

het traceren moesten persoonsgegevens (persoonlijke contacten, gsm-gegevens/e-mails, bezochte plaatsen enzovoort) worden verzameld, die vervolgens moesten worden gekruist met de gegevens van de databanken van de overheidsinstellingen (bijvoorbeeld inzake gezondheidszorg of de RSZ). Voor het aanleggen van databanken voor de vaccinatie en inzake ziektesymptomen moeten persoonlijke gezondheidsgegevens worden vergaard, verwerkt, opgeslagen of meegedeeld. Zo bundelt de Kruispuntbank van de Sociale Zekerheid (KSZ) heel wat COVID-19-gerelateerde gegevens (contact-, identificatie-, werk- en verblijfsgegevens) van de werknemers en de zelfstandigen. Van die gegevens wordt tevens voor het eerst gebruik gemaakt bij de telegeneeskunde, een dienstverlening die door de pandemie een boost heeft gekregen.

Door die initiatieven inzake gegevensvergaring en -koppeling is het probleem er niet bepaald minder delicaat op geworden. Hoewel al die initiatieven gericht zijn op gezondheidsdoeleinden van algemeen belang, moet de algemene verordening gegevensbescherming (AVG) worden geëerbiedigd en moeten het doel van de verwerking van de persoonsgegevens en het evenredigheidsbeginsel nauwkeurig worden omschreven. De regeling moet nog steeds zijn gegrondvest op een passende, ter zake dienende en niet-overmatige gegevensverwerking die in verhouding staat tot de nagestreefde doeleinden. De onmisbare randvoorwaarden ter waarborging van de bescherming van de persoonlijke levenssfeer moeten op democratische wijze worden gedefinieerd, besproken en aangenomen. Elke afwijking van die voorwaarden doet afbreuk aan de bescherming van de privacy en van de persoonsgegevens. De technieken inzake gegevenskoppeling (*data matching)* en -onderzoek (*data mining)* door middel van algoritmen kunnen namelijk leiden tot doorgedreven vormen van *profiling* en ernstige misstanden[2]. Om ervoor te zorgen dat de burger erop kan vertrouwen dat de overheid de databanken goed beheert, moeten de gegevens dan ook op voorbeeldige wijze worden beheerd en verwerkt.

In België wordt gewerkt met een gedecentraliseerd gegevensbeheermodel, waarbij de gegevens zijn opgeslagen in verschillende databanken die uit voorzorg los

[2] L'Autorité de protection des données (APD) a introduit un recours en annulation auprès du Conseil d'État contre l'arrêté ministériel du 12 janvier 2021 modifiant l'arrêté ministériel du 28 octobre 2020 portant des mesures d'urgence pour limiter la propagation du coronavirus COVID-19 habilitant, en son article 8, l'ONSS à avoir recours aux techniques de data matching et de data mining.

[2] De Gegevensbeschermingsautoriteit (GBA) heeft bij de Raad van State een beroep tot vernietiging ingesteld tegen het ministerieel besluit van 12 januari 2021 houdende wijziging van het ministerieel besluit van 28 oktober 2020 houdende dringende maatregelen om de verspreiding van het coronavirus COVID-19 te beperken, dat krachtens artikel 8 de RSZ machtigt gebruik te maken van *data matching*- en *data mining*-technieken.

rendues, par prudence, indépendantes les unes des autres (ce que l'on appelle les sources authentiques[3]). Les données de santé sont principalement regroupées au sein de la Banque Carrefour de la Sécurité Sociale, dont les missions sont encadrées par une loi. Cette architecture a l'avantage de protéger les données contre le piratage. La multiplication des croisements de données tend à mettre en place un système de plus en plus centralisé.

Les croisements de données issues de sources différentes et normalement indépendantes nécessitent une grande prudence et un encadrement légal renforcé. Ils doivent faire l'objet d'une demande préalable comprenant la description des croisements envisagés, une justification précise et fondée quant à leur finalité, la description des personnes habilitées à avoir accès aux données croisées et la fixation de la durée de l'autorisation.

Pour les citoyens, faire confiance à un système qui gère des données sensibles signifie avoir la certitude que les données sont exclusivement utilisées par les personnes dûment habilitées, dans un but déterminé et en respectant le principe de transparence du RGPD.

Les plateformes telles que eHealth (Institution publique fédérale ayant pour mission de promouvoir et de soutenir une prestation de services et un échange d'informations électroniques mutuels entre tous les acteurs des soins de santé), Healthdata.be (enregistrement et conservation de données de santé fournies par divers prestataires de soins), mhealthbelgium.be, Masanté.be, Mijngezondheid.be, Réseau Santé Wallon et Collaboratief Zorgplatform (CoZo), les organismes tels que la Banque Carrefour de la Sécurité Sociale, les mutualités, la Société de Mécanographie pour l'Application des Lois Sociales (Smals) et EGOV Select ou encore le programme G-Cloud visant à mettre en place une infrastructure ICT au bénéfice des institutions publiques, sont autant de lieux d'utilisation de données à caractère personnel sensibles.

Quels sont les sources, les types et les buts du traitement des données à caractère personnel de santé gérées par ces plateformes, organismes et programme G-Cloud? Quels sont les contrôles internes et externes exercés? Qui siège dans ces organismes? Les citoyens sont-ils suffisamment informés sur les traitements effectués?

[3] Loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral, Art. 2., 6° "" source authentique ": banque de données dans laquelle sont conservées des données authentiques;" - Art. 2., 5° "" donnée authentique ": donnée récoltée et gérée par une instance dans une base de données et qui fait foi comme donnée unique et originale concernant la personne ou le fait de droit concerné, (…).".

van elkaar staan (zogenaamde authentieke bronnen[3]). De gezondheidsgegevens worden hoofdzakelijk gebundeld in de Kruispuntbank van de Sociale Zekerheid, waarvan het takenpakket wettelijk is bepaald. Die architectuur biedt het voordeel dat de gegevens tegen piraterij zijn beschermd. Door de toenemende kruising van gegevens wordt het systeem almaar meer gecentraliseerd.

De kruising van gegevens uit verschillende en normaliter onafhankelijke bronnen vereist een grote behoedzaamheid en een strikter rechtskader. Voor dergelijke verrichtingen moet vooraf een aanvraag worden ingediend waarin de beoogde kruising wordt omschreven, de bedoeling ervan nauwkeurig en gefundeerd wordt verantwoord, wordt aangegeven wie gemachtigd is om toegang te hebben tot de gekruiste gegevens en de duur van de machtiging wordt bepaald.

Vertrouwen stellen in een systeem dat gevoelige gegevens beheert, houdt voor de burgers in dat zij de zekerheid hebben dat de gegevens uitsluitend door naar behoren gemachtigde personen worden gebruikt voor een welbepaald doel en met naleving van het transparantiebeginsel dat is vervat in de AVG.

Platforms zoals *eHealth* (een federale overheidsinstelling die werd opgedragen de elektronische dienstverlening en informatie-uitwisseling tussen alle gezondheidszorgactoren te bevorderen en te ondersteunen), *Healthdata.be* (de registratie en opslag van gezondheidsgegevens die door diverse zorgverleners worden aangeleverd), *mhealthbelgium.be*, *Masanté.be*, Mijngezondheid.be, het *Réseau Santé Wallon* en het Collaboratief Zorgplatform (CoZo), instanties zoals de Kruispuntbank van de Sociale Zekerheid, de ziekenfondsen, de Maatschappij voor mecanografie ter toepassing van de sociale wetten (MvM) en Egov Select, of nog het G-Cloud-programma, dat ertoe strekt een ICT-infrastructuur ten behoeve van de overheidsinstellingen uit te werken, maken allemaal gebruik van gevoelige persoonsgegevens.

De vraag rijst vanwaar de door die platforms, instanties en het G-Cloud-programma beheerde persoonlijke gezondheidsgegevens afkomstig zijn, om welk soort van gegevens het gaat en met welk doel zij worden verwerkt. Hoe staat met de interne en de externe controle? Wie heeft zitting in die instanties? Zijn de burgers voldoende geïnformeerd over de verwerkingen die worden uitgevoerd?

[3] Zie de wet van 15 augustus 2012 houdende oprichting en organisatie van een federale dienstenintegrator, artikel 2, 6°: ""authentieke bron": gegevensbank waarin authentieke gegevens gehouden worden;", alsmede artikel 2, 5°: ""authentiek gegeven": gegeven dat door een instantie ingezameld en beheerd wordt in een gegevensbank en geldt als uniek en oorspronkelijk gegeven over de desbetreffende persoon of rechtsfeit (…);".

Si le système belge a été pensé au départ dans le but de sécuriser au maximum les données des patients, on constate aujourd'hui qu'il est devenu trop complexe, peu lisible, opaque et, dès lors, sujet à défiance.

Le meilleur moyen de rétablir la confiance serait de permettre à chaque citoyen d'accéder à l'ensemble des données de santé le concernant dont l'État dispose, à l'instar de l'espace Myminfin.be[4]. Le système doit aussi se placer dans une démarche de service rendu à l'usager: suivi digital des carnets de vaccination[5], prescriptions électroniques, etc. Chaque citoyen doit être informé de l'existence des banques de données et des réseaux d'échanges de ces données avant que ses données y soient intégrées et devrait en principe donner son consentement explicite ayant trait à l'introduction de ses données à caractère personnel au sein de ces banques et réseaux. Mais comment ces notions d'information, de légalité et de consentement sont-elles concrétisées? C'est trop souvent l'adage "qui ne dit mot, consent" qui s'applique en ces matières.

Nous pensons dès lors qu'à côté d'un cadre législatif, il faut un cadre de gouvernance de ces données et des organismes publics et privés qui les gèrent, ce qui implique un contrôle interne et externe.

Concernant le système de santé, la défiance supplémentaire de la population vis-à-vis des groupes technologiques et pharmaceutiques qui pourraient avoir accès aux banques de données dans le but de les exploiter pour réaliser du profit, risque de faire perdre toute confiance dans le système et dans les acteurs de la santé. C'est pourquoi l'utilisation des données doit uniquement être motivée par l'intérêt général et – surtout – l'intérêt des patients et, plus largement, des usagers de soins et des services de santé, et ce dans le cadre strict du RGPD.

Par intérêt général, nous considérons notamment l'amélioration de la qualité, de la sécurité et de la réactivité des services de santé, l'anticipation et la réduction des risques liés à la santé publique, la recherche et le développement d'outils de diagnostic et de traitements nouveaux dans un cadre transparent et éclairé, la promotion et la prévention, la gestion efficiente des ressources de la santé, l'amélioration de la planification

Hoewel bij het uitwerken van de Belgische regeling werd beoogd de patiëntengegevens maximaal te beveiligen, wordt thans vastgesteld dat ze te complex, nauwelijks bevattelijk en hermetisch is, en bijgevolg wantrouwen opwekt.

De beste manier om het vertrouwen te herstellen, zou erin bestaan elke burger toegang te bieden tot al zijn gezondheidsgegevens waarover de overheid beschikt, naar het voorbeeld van Myminfin.be[4]. Het systeem moet tevens worden opgevat als een vorm van dienstverlening aan de gebruiker; hij zou bijvoorbeeld zijn vaccinatiestatus elektronisch kunnen opvolgen[5], elektronische voorschriften krijgen enzovoort. Elke burger moet worden geïnformeerd over het bestaan van de databanken en van de informatie-uitwisselingsnetwerken voordat zijn gegevens erin worden opgenomen. In principe zou hij uitdrukkelijk moeten instemmen met de opname van zijn persoonsgegevens in die databanken en netwerken. De vraag rijst echter hoe die begrippen "informatie", "wettigheid" en "toestemming" concreet worden ingevuld. Ter zake wordt al te vaak het principe "zwijgen is toestemmen" gehanteerd.

De indieners van dit voorstel van resolutie zijn derhalve van oordeel dat men naast een wetgevend kader ook nood heeft aan een raamwerk voor het beheer van die gegevens en voor de openbare en private instellingen die ze beheren. Daartoe moet in zowel interne als externe controle worden voorzien.

Voor het gezondheidssysteem geldt bovendien dat alle vertrouwen in het systeem en in de gezondheidszorgactoren dreigt teniet te worden gedaan door het bijkomende wantrouwen van de bevolking jegens de technologische en farmaceutische consortia waaraan toegang tot de databanken zou kunnen worden verleend om er winst uit te slaan. Daarom mag het gebruik van de gegevens alleen worden ingegeven door het algemeen belang, vooral dat van de patiënten, en meer algemeen door dat van de gebruikers van de gezondheidszorg en -diensten. Bovendien mogen die gegevens enkel binnen het strikte kader van de AVG worden gebruikt.

In het kader van het algemeen belang moet in dezen inzonderheid worden gelet op de verbetering van de kwaliteit, de veiligheid en het reactievermogen van de gezondheidsdiensten, alsook op het anticiperen op en de vermindering van de risico's voor de volksgezondheid. Tevens moet worden ingezet op het onderzoek naar en de ontwikkeling van diagnostische hulpmiddelen en nieuwe behandelingen binnen een transparant en

4 Sans couplage opéré avec les données fiscales évidemment.

5 La plateforme Vaccinnet développée par Kind&Gezin n'est pas [encore] intégrée aux réseaux de santé wallons et bruxellois.

4 Uiteraard zonder koppeling aan de fiscale gegevens.

5 Het Vaccinnet-platform dat door Kind&Gezin werd ontwikkeld, is (nog) niet gelinkt met de Waalse en Brusselse gezondheidsnetwerken.

et l'évaluation des politiques publiques, l'élaboration de stratégies de politiques de santé publique, la réduction des inégalités de santé, l'action sur les déterminants de la santé et – surtout – l'amélioration de l'implication des patients dans les soins et leur vécu à cet égard.

Ces axes inhérents à toute vision de santé publique sont essentiels pour atteindre des objectifs de santé pour toutes et tous mais de tels axes doivent être connus, compris et partagés. Il s'agit dès lors que les pouvoirs publics contribuent à contrôler le respect des législations et politiques publiques relatives à la protection de la vie privée. Cela signifie qu'il est nécessaire d'élaborer et de mettre en œuvre de manière rigoureuse un cadre solide de gouvernance en matière de données de santé, protecteur de la vie privée, garantissant la sécurité et nécessitant la détermination et la gestion des risques.

Le 13 décembre 2016, sur proposition du Comité de la santé et du Comité de la politique de l'économie numérique, l'OCDE a adopté une recommandation[6] exhortant les pays membres à adopter un cadre global de gouvernance afin d'encourager la mise à disposition et l'utilisation des données à caractère personnel de santé à des fins sanitaires servant l'intérêt général et, dans le même temps, afin d'amplifier les mécanismes de protection de la vie privée, des données personnelles de santé et de sécurité des données.

La définition et la mise en place d'un cadre national de gouvernance des données de santé est une opportunité pour la Belgique de mettre à plat le cadastre des données existantes, les interactions entre elles et d'évaluer l'opportunité et la proportionnalité dans l'exploitation des données à caractère personnel de santé à des fins répondant à l'intérêt public, par exemple dans la lutte contre la pandémie de COVID-19. La présente proposition de résolution reprend une large part des balises mises en exergue dans la recommandation de l'OCDE[7].

6 OCDE, Recommandation du Conseil sur la gouvernance des données de santé, OECD/LEGAL/0433.

7 OCDE, op.cit..

geïnformeerd kader, op gezondheidsbevordering en -preventie, en op een efficiënt beheer van de gezondheidszorgmiddelen. Daartoe moeten de planning en de evaluatie van het overheidsbeleid worden verbeterd en moeten strategieën voor het volksgezondheidsbeleid worden uitgewerkt. Voorts moet de ongelijkheid op het vlak van gezondheid worden teruggedrongen door in te spelen op de factoren die de gezondheid bepalen. Bovenal moeten de patiënten meer bij de zorg worden betrokken en moet er meer aandacht gaan naar hoe zij die zorg ervaren.

Die beleidslijnen die als een rode draad door elke visie op volksgezondheid lopen, zijn van wezenlijk belang om de gezondheidsdoelstellingen voor alle burgers te verwezenlijken, maar dan moeten ze ook gekend zijn, begrepen en gedeeld worden. Daarom moeten de overheden meewerken aan de controle van de naleving van de wetgevingen en van het overheidsbeleid inzake de bescherming van het privéleven. Dit houdt in dat een degelijk raamwerk voor het beheer van de gezondheidsgegevens moet worden uitgewerkt en nauwgezet moet worden geïmplementeerd, dat garant staat voor de bescherming van het privéleven en de veiligheid van de gegevens. Zulks vereist dat de risico's worden omschreven en beheerd.

Op voorstel van het *Health Committee* en van het *Committee on Digital Economy Policy* heeft de OESO op 13 december 2016 een aanbeveling aangenomen[6], waarin de lidstaten ertoe werden opgeroepen een algemeen raamwerk voor het beheer in te stellen om persoonlijke gezondheidsgegevens toegankelijker te maken en te gebruiken voor gezondheidsdoeleinden van algemeen belang, en tegelijk de mechanismen ter bescherming van het privéleven, van de persoonlijke gezondheidsgegevens en van de veiligheid van de gegevens uit te bouwen.

Bij het uitwerken en implementeren van een nationaal raamwerk voor het beheer van de gezondheidsgegevens kan België de gelegenheid benutten om het kadaster van de bestaande gegevens en de onderlinge interacties tussen die gegevens te herijken. Ook de wenselijkheid van en de evenredigheid bij het gebruik van de persoonlijke gezondheidsgegevens voor doelstellingen van algemeen belang kunnen in dat verband tegen het licht worden gehouden, bijvoorbeeld in het kader van de bestrijding van de COVID-19-pandemie. Dit voorliggende voorstel van resolutie ligt grotendeels in de lijn van de bakens die in de OESO[7].-aanbeveling werden uitgezet.

6 OESO, *Recommendation of the Council on Health Data Governance*, OECD/LEGAL/0433.

7 OESO, *ibidem*.

De même, en Belgique, la gestion des données dans le contexte de la crise sanitaire du coronavirus est critiquée par les professionnels du droit, les experts de l'Autorité de protection des données, les avis du Conseil d'État ou encore les associations luttant pour les droits de l'homme[8]. Des problèmes de fond mais aussi d'indépendance sont pointés du doigt.

Récemment, c'est un projet du domaine privé, "Putting data at the center", qui a fait l'objet de critiques tant sur le plan de la méthode que de la gouvernance[9]. En effet, selon certaines révélations parues dans la presse, ce projet aurait pour objectif de constituer un véritable carrefour de toute une série de bases de données concernant les citoyens et les entreprises. L'opération qui consiste à croiser les données sociales, de santé et fiscales semble échapper à tout contrôle démocratique et ne pas se conformer à la loi.

In fine, au vu de tous ces éléments, les signataires de la présente proposition de résolution demandent au gouvernement d'étudier le paysage belge de la gestion des données afin d'y corriger les imprécisions et de lever les imperfections. Il est essentiel de renforcer la gestion des données personnelles (de santé, notamment) afin que les thèmes liés à la gouvernance et au traitement des données soient conformes aux exigences démocratiques et éthiques eu égard aux normes les plus strictes en la matière.

Laurence HENNUY (Ecolo-Groen)
Barbara CREEMERS (Ecolo-Groen)
Cécile THIBAUT (Ecolo-Groen)
Stefaan VAN HECKE (Ecolo-Groen)
Gilles VANDEN BURRE (Ecolo-Groen)
Marie-Colline LEROY (Ecolo-Groen)
Séverine de LAVELEYE (Ecolo-Groen)
Evita WILLAERT (Ecolo-Groen)
Guillaume DEFOSSÉ (Ecolo-Groen)
Kristof CALVO (Ecolo-Groen)

In België wordt ook het gegevensbeheer in de context van de COVID-19-gezondheidscrisis op de korrel genomen door rechtsbeoefenaars, experten van de Gegevensbeschermingsautoriteit, in de adviezen van de Raad van State, of nog door mensenrechtenorganisaties[8]. In dat verband wordt zowel op inhoudelijke problemen gewezen als op problemen inzake onafhankelijkheid.

Onlangs nog kreeg het privéproject "*Putting data at the center*" kritiek, zowel op methodologisch vlak als op het vlak van *governance*[9]. Volgens diverse persberichten zou dit project immers beogen te voorzien in een echt kruispunt van heel wat databanken die gegevens van burgers en bedrijven bevatten. Dit initiatief tot kruising van sociale, fiscale en gezondheidsgegevens lijkt aan geen enkele democratische controle onderworpen te zijn en in strijd te zijn met de wet.

In het licht van al deze elementen verzoeken de indieners van dit voorstel van resolutie de regering *in fine* het Belgische landschap van het gegevensbeheer onder de loep te nemen om de onduidelijkheden en de manco's weg te werken. Het is van wezenlijk belang dat het beheer van de persoonsgegevens (meer bepaald betreffende de gezondheid) wordt uitgebouwd, om de *governance* en de verwerking ervan te doen sporen met de democratische en ethische vereisten, gezien de zeer strikte normen ter zake.

8 "La Ligue des droits humains veut l'annulation d'un arrêté ministériel", 11 février 2021, disponible sur *https://plus.lesoir.be/354642/article/2021-02-11/vie-privee-la-ligue-des-droits-humains-veut-lannulation-dun-arrete-ministeriel*.

9 Voy. "Le Parlement doit reprendre la main sur la gestion des données des Belges", 10 mars 2021, disponible sur *https://plus.lesoir.be/359834/article/2021-03-10/le-parlement-doit-reprendre-la-main-sur-la-gestion-des-donnees-des-belges*; "Un projet sans contrôle de l'État pour profiler les Belges", 10 mars 2021, disponible sur *https://plus.lesoir.be/359783/article/2021-03-10/vie-privee-un-projet-sans-controle-de-letat-pour-profiler-les-belges*.

8 *"La Ligue des droits humains veut l'annulation d'un arrêté ministériel"*, 11 februari 2021, beschikbaar via *https://plus.lesoir.be/354642/article/2021-02-11/vie-privee-la-ligue-des-droits-humains-veut-lannulation-dun-arrete-ministeriel*.

9 "*Le Parlement doit reprendre la main sur la gestion des données des Belges"*, 10 maart 2021, beschikbaar via *https://plus.lesoir.be/359834/article/2021-03-10/le-parlement-doit-reprendre-la-main-sur-la-gestion-des-donnees-des-belges*; *"Un projet sans contrôle de l'État pour profiler les Belges*", 10 maart 2021, beschikbaar via *https://plus.lesoir.be/359783/article/2021-03-10/vie-privee-un-projet-sans-controle-de-letat-pour-profiler-les-belges*.

PROPOSITION DE RÉSOLUTION

La Chambre des représentants,

A. vu l'article 12 de la Déclaration universelle des droits de l'homme, selon lequel "Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation"10;

B. vu l'article 8 de la Convention européenne des droits de l'homme, selon lequel "Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance" et "Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire (…)"11;

C. vu l'article 7 de la Charte des droits fondamentaux de l'Union européenne, selon lequel "Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications"12;

D. vu l'article 22 de la Constitution belge, selon lequel "Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi";

E. vu le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données - RGPD) et la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel;

F. vu la loi du 11 avril 1994 relative à la publicité de l'administration13;

G. vu la loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

10 *https://www.un.org/fr/universal-declaration-human-rights/.*

11 *https://www.echr.coe.int/Documents/Convention_FRA.pdf.*

12 *https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN.*

13 *https://www.ejustice.just.fgov.be/cgi_loi/change_lg_2.pl?language=fr&nm=1994000357&la=F.*

VOORSTEL VAN RESOLUTIE

De Kamer van volksvertegenwoordigers,

A. gelet op artikel 12 van de Universele Verklaring van de Rechten van de Mens, dat stelt dat "Niemand zal onderworpen worden aan willekeurige inmenging in zijn persoonlijke aangelegenheden, in zijn gezin, zijn tehuis of zijn briefwisseling, noch aan enige aantasting van zijn eer of goede naam"10;

B. gelet op artikel 8 van het Europees Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden, dat stelt dat "Een ieder (…) recht [heeft] op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie" en dat "Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is (…)"11;

C. gelet op artikel 7 van het Handvest van de grondrechten van de Europese Unie, dat stelt dat "Eenieder (…) recht [heeft] op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie"12;

D. gelet op artikel 22 van de Belgische Grondwet, dat stelt dat "Ieder (…) recht [heeft] op eerbiediging van zijn privéleven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald";

E. gelet op Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (algemene verordening gegevensbescherming - AVG), alsmede op de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens;

F. gelet op de wet van 11 april 1994 betreffende de openbaarheid van bestuur13;

G. gelet op de wet van 5 september 2018 tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van verordening (EU) 2016/679 van 27 april 2016 van het Europees

10 *https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=dut.*

11 *https://www.echr.coe.int/documents/convention_nld.pdf.*

12 *https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN.*

13 *https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=1994041151&table_name=wet.*

relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)[14];

H. considérant que les données à caractère personnel de santé sont les données les plus sensibles en matière de vie privée et que, par conséquent, toutes les garanties nécessaires doivent être prises lors de leur traitement tant légalement qu'opérationnellement;

I. considérant que l'accès aux données à caractère personnel de santé et leur traitement peuvent servir l'intérêt sanitaire général et offrir des avantages importants aux individus et à la société;

J. considérant le principe de légalité en vertu duquel tout traitement de données qui implique une ingérence importante dans la vie des citoyens doit être prévu par une norme législative détaillant de manière claire et exhaustive ses éléments essentiels (données traitées, personnes concernées, finalité et responsable du traitement, durée de conservation, etc.);

K. considérant que les systèmes de santé gèrent un volume sans cesse croissant de données à caractère personnel de santé, que bien que ces données soient détenues de manière cloisonnée par les organismes et les autorités qui les recueillent et que lorsqu'un transfert, une mise en correspondance et une analyse des données de santé sont effectués, le principe de proportionnalité et la finalité de traitement de ces données au service d'objectifs sanitaires répondant à l'intérêt de la collectivité s'accroît sensiblement;

L. considérant que la confiance du public à l'égard de la protection des données à caractère personnel de santé doit être préservée et que cette confiance se gagne par la transparence, le contrôle et le respect strict des législations et politiques publiques relatives à la protection de la vie privée;

M. considérant que les données à caractère personnel de santé, étant de nature sensible et soumises à des normes éthiques et au principe du secret médical, exigent un degré particulièrement élevé de protection et que l'évolution technologique peut à la fois permettre un usage de ces données qui respecte la vie privée mais

[14] *https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2018090501&table_name=loi#:~:text=Par%20d%C3 %A9rogation%20aux%20dispositions%20de,par%20la%20Chambre%20des%20repr%C3 %A9sentants*.

Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG[14] (algemene verordening gegevensbescherming);

H. overwegende dat, wat de persoonlijke levenssfeer betreft, geen gegevens zo heikel zijn als de persoonsgegevens betreffende de gezondheid, en dat bij hun verwerking bijgevolg alle nodige wettelijke en operationele waarborgen moeten worden verstrekt;

I. overwegende dat de toegang tot de persoonlijke gezondheidsgegevens en de verwerking ervan het algemeen volksgezondheidsbelang kunnen dienen en zowel de burgers als de samenleving belangrijke voordelen kunnen bieden;

J. gelet op het wettigheidsbeginsel, op grond waarvan elke gegevensverwerking die een ingrijpende inmenging in het leven van de burgers impliceert, moet gebeuren op basis van een wetgevende norm die op duidelijke en exhaustieve wijze de wezenlijke aspecten van die verwerking bepaalt (de verwerkte gegevens, de betrokken personen, de finaliteit van en de verantwoordelijke voor de verwerking, de duur van de bewaring enzovoort);

K. overwegende dat de gezondheidssystemen een almaar groter volume aan persoonlijke gezondheidsgegevens beheren en dat, ondanks het feit dat die gegevens los van elkaar worden beheerd door de verzamelende instellingen en overheden en dat zij bij de overheveling ervan op elkaar worden afgestemd en geanalyseerd, het evenredigheidsbeginsel en het doel van de verwerking van die gegevens ten dienste van gezondheidsdoelen die het openbaar belang dienen, aanzienlijk aan belang winnen;

L. overwegende dat het vertrouwen van het brede publiek ten aanzien van de bescherming van persoonlijke gezondheidsgegevens moet worden gehandhaafd en dat dit vertrouwen wordt verdiend door middel van transparantie, toezicht en de strikte inachtneming van de wetgevingen en beleidsmaatregelen met betrekking tot de bescherming van de persoonlijke levenssfeer;

M. overwegende dat de persoonlijke gezondheidsgegevens, die van nature heikel zijn en aan ethische normen, alsook aan het beginsel van het medisch beroepsgeheim zijn onderworpen, een uitermate hoge beschermingsgraad vergen, en dat de technologische evolutie kan leiden tot een gebruik van die gegevens dat acht slaat

[14] *https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2018090501&table_name=wet*.

aussi générer de nouveaux risques pour la vie privée et la sécurité des données;

N. considérant que l'utilisation des données de santé nécessite d'élaborer et de mettre en œuvre de manière rigoureuse un cadre de gouvernance des données de santé solide, adapté à la situation et protecteur de la vie privée, ce qui nécessite la détermination et la gestion des risques pour la vie privée et la sécurité;

O. considérant que la défense de l'intérêt général constitue une fonction importante incombant aux gouvernements et que la gouvernance des données de santé n'est pas le domaine réservé du gouvernement fédéral mais qu'elle concerne tous les niveaux de pouvoir;

P. considérant que les données de santé (examens et protocoles médicaux, données de laboratoire, données relatives aux médicaments et aux vaccins, etc.) ne peuvent être mises à la disposition des prestataires de soins que dans une optique de transparence et de coopération, que chaque citoyen doit savoir que ses données de santé sont rassemblées dans des bases de données spécifiques, y consentir et doit pouvoir y avoir accès pour consulter ses propres données, les utiliser pour s'informer, améliorer le dialogue avec les professionnels de santé ou aider ses proches à gérer leurs maladies éventuelles;

Q. considérant que les autorités de santé publique doivent non seulement se munir d'outils et de moyens nécessaires pour empêcher la marchandisation des soins de santé et la commercialisation non contrôlée des données médicales, mais aussi viser la recherche et le développement en matière de santé publique dans un cadre transparent et contrôlé;

R. considérant que les données traitées dans le cadre de la lutte contre le COVID-19 sont principalement des données de santé, que leur collecte et traitement se sont accélérés et que toutes les garanties nécessaires doivent être prises tant légalement qu'opérationnellement, mais que, dans une situation de pandémie, des données de santé sont aussi à l'origine de mesures limitant les libertés de mouvement et de rassemblement des citoyens et citoyennes afin de protéger l'ensemble de la population, ce qui requiert une vigilance accrue en ce qui concerne la protection des données;

S. considérant la nécessité pour la Belgique d'exposer de manière exhaustive le cadastre des banques de

op de persoonlijke levenssfeer, maar evengoed nieuwe gevaren in het leven kan roepen wat de persoonlijke levenssfeer en de veiligheid van de gegevens betreft;

N. overwegende dat het gebruik van de gezondheidsgegevens vereist dat daartoe een raamwerk voor het beheer van de gezondheidsgegevens wordt uitgewerkt en nauwlettend wordt uitgerold, dat bovendien aan de situatie is aangepast en acht slaat op de persoonlijke levenssfeer, wat betekent dat de risico's op het vlak van de persoonlijke levenssfeer en van de veiligheid van de gegevens moeten worden geïdentificeerd en beheerd;

O. overwegende dat het behartigen van het algemeen belang een belangrijke taak van de regeringen is, alsook dat het beheren van de gezondheidsgegevens het werkterrein van de federale regering overstijgt en álle beleidsniveaus aanbelangt;

P. overwegende dat de gezondheidsgegevens (medische onderzoeken en protocollen, laboratoriumresultaten, gegevens over geneesmiddelen en vaccinaties enzovoort) de zorgverstrekkers alleen ter beschikking mogen worden gesteld voor transparantie- en samenwerkingsdoeleinden, dat elke burger ervan in kennis moet worden gesteld dat zijn gezondheidsgegevens in specifieke gegevensbanken worden bewaard, daarmee moet instemmen, inzage moet kunnen hebben in zijn eigen gegevens en deze moet kunnen aanwenden om zich te informeren, beter in dialoog te treden met de zorgverstrekkers of zijn naasten met eventuele aandoeningen te kunnen bijstaan;

Q. overwegende dat de volksgezondheidsinstanties niet alleen over de nodige instrumenten en middelen moeten beschikken om het verhandelen van de gezondheidszorg en de ongebreidelde commercialisering van medische gegevens te voorkomen, maar ook moeten inzetten op onderzoek en ontwikkeling inzake volksgezondheid, in een duidelijk en gecontroleerd raamwerk;

R. overwegende dat in het raam van de strijd tegen COVID-19 hoofdzakelijk gezondheidsgegevens worden verwerkt, dat die gegevens almaar sneller worden verzameld en verwerkt en dat alle nodige wettelijke en operationele waarborgen moeten worden verstrekt, maar dat gezondheidsgegevens in de context van een pandemie tegelijk ten grondslag liggen aan maatregelen die de vrijheid van beweging en van vergadering van de burgers inperken om de hele bevolking te beschermen, wat inzake gegevensbescherming extra waakzaamheid vereist;

S. overwegende dat de Belgische overheid exhaustieve informatie moet verstrekken over de bestaande

données existantes, les interactions entre elles et les organisations qui les gèrent;

T. considérant la nécessité d'évaluer l'opportunité et la proportionnalité de l'exploitation des données à caractère personnel de santé dans un cadre particulier comme la lutte contre la pandémie de COVID-19 et, plus largement, de toute autre pandémie;

U. considérant les révélations par la presse du projet "*Putting data at the center*" et le manque de transparence autour de celui-ci;

V. considérant que les techniques de profilage présentent des risques sérieux de dérives et d'infractions aux normes supranationales et nationales précitées;

W. considérant les problèmes d'indépendance soulevés en particulier par l'Autorité de protection des données, par les professionnels du droit et les associations qui luttent pour les droits de l'homme;

X. considérant l'urgence et la nécessité d'étudier en profondeur la trajectoire des données à caractère personnel et le paysage belge de la gestion des bases de données;

Y. considérant le rôle contesté du comité de sécurité de l'information (CSI) depuis sa mise en place, notamment par le Conseil d'État, ainsi que de ses délibérations par lesquelles il autorise des transmissions de données, se substituant ainsi au Parlement;

Z. considérant les déclarations de M. M. Michel, secrétaire d'État à la Digitalisation, chargé de la Simplification administrative, de la Protection de la vie privée et de la Régie des bâtiments, adjoint au Premier ministre, quant à sa volonté d'avancer concernant le travail portant sur la transparence des données à caractère personnel[15];

DEMANDE AU GOUVERNEMENT FÉDÉRAL:

1. d'établir et de mettre en œuvre un cadre national de gouvernance des données de santé afin d'encourager la disponibilité et l'utilisation des données à caractère personnel de santé à des fins sanitaires au service de l'intérêt général, tout en favorisant la protection de la vie privée, la protection des données personnelles de

[15] "Profiler les Belges? L'exécutif en défense, les députés à l'attaque", Le Soir, 11 mars 2021, disponible sur *https://plus.lesoir.be/art/d-20210310-GLNM11*.

gegevensbanken, over de koppelingen tussen die gegevensbanken en over de organisaties die deze gegevensbanken beheren;

T. overwegende dat het gebruik van persoonlijke gezondheidsgegevens in de specifieke context van de strijd tegen de COVID-19-pandemie en, meer algemeen, tegen enige andere pandemie, moet worden getoetst op zijn wenselijkheid en evenredigheid;

U. gelet op de onthullingen in de media omtrent het project "*Putting data at the center*" en op het gebrek aan transparantie daaromtrent;

V. gelet op het risico dat de *profiling*-technieken zullen leiden tot ernstige uitwassen en tot inbreuken op de voormelde nationale en supranationale normen;

W. gelet op de pijnpunten in verband met de onafhankelijkheid die onder de aandacht zijn gebracht door met name de Gegevensbeschermingsautoriteit, de rechtsbeoefenaars en de mensenrechtenverenigingen;

X. overwegende dat dringend diepgaand onderzoek moet worden verricht naar het verkeer van persoonsgegevens en dat het gegevensbankenbeheer in België terdege in kaart moet worden gebracht;

Y. gelet op de rol van het Informatieveiligheidscomité (IVC) die sinds de oprichting ervan wordt aangevochten, met name door de Raad van State, en op de door het IVC gevoerde beraadslagingen op basis waarvan de overdracht van gegevens wordt toegestaan en waardoor het IVC zich in de plaats stelt van het Parlement;

Z. gelet op de verklaringen van de heer M. Michel, staatssecretaris voor Digitalisering, belast met Administratieve Vereenvoudiging, Privacy en met de Regie der Gebouwen, toegevoegd aan de eerste minister, omtrent zijn voornemen vooruitgang te boeken inzake de transparantie van persoonsgegevens[15];

VERZOEKT DE FEDERALE REGERING:

1. een nationaal raamwerk voor het beheer van gezondheidsgegevens uit te tekenen en uit te rollen, teneinde persoonlijke gezondheidsgegevens vlotter beschikbaar te doen stellen en te doen aanwenden voor gezondheidsdoeleinden ten dienste van het algemeen belang, en tegelijk de bescherming van de persoonlijke

[15] *Profiler les Belges? L'exécutif en défense, les députés à l'attaque*, *Le Soir*, 11 maart 2021, beschikbaar op *https://plus.lesoir.be/art/d-20210310-GLNM11*.

santé et tout en garantissant la sécurité des données. Ce cadre devra prévoir:

a) l'engagement et la participation, notamment par la consultation du public, d'un large éventail de parties prenantes (Conseil d'État, Autorité de protection des données, Institut Fédéral pour la Protection et la Promotion des Droits Humains, associations de patients, etc.) afin de veiller à ce que le traitement des données à caractère personnel de santé serve l'intérêt général et soit conforme au règlement général sur la protection des données (RGPD), aux valeurs de la société et aux attentes raisonnables des personnes physiques, tant pour ce qui est de la protection de leurs données que de l'utilisation de ces données à des fins de gestion du système de santé, de recherche, de statistique ou d'autres objectifs sanitaires répondant à l'intérêt général;

b) une coordination interfédérale et la promotion de la coopération entre les organismes chargés du traitement des données personnelles de santé, qu'ils soient publics ou privés. Cette coordination s'inscrit nécessairement dans le cadre de plans interfédéraux ou nationaux de politique de santé publique[16].

Cette coopération devra encourager des éléments et des formats de données communs, l'assurance de la qualité ainsi que des normes d'interopérabilité des données, des politiques et des procédures communes favorisant un partage de données qui soit contrôlé et transparent à des fins de gestion du système de santé, de recherche, de statistique ou d'autres objectifs sanitaires répondant à l'intérêt général tout en protégeant la vie privée et en garantissant la sécurité des données;

2. de décrire, documenter et d'examiner les capacités des systèmes de données de santé du secteur public utilisés pour traiter les données à caractère personnel de santé afin de servir et de protéger l'intérêt général. Cet examen devra porter sur:

a) la disponibilité, la qualité, l'adéquation et l'accessibilité des données, ainsi que sur la protection de la vie privée et la sécurité des données;

[16] Par exemple: plan cancer, plan assuétudes, plan vaccination.

levenssfeer en van de persoonlijke gezondheidsgegevens te bevorderen, alsook de veiligheid van de gegevens te waarborgen. Dat raamwerk behelst:

a) de betrokkenheid en de deelname, meer bepaald via een raadpleging van het publiek, van een breed scala aan stakeholders (de Raad van State, de Gegevensbeschermingsautoriteit, het Federaal Instituut voor de bescherming en de bevordering van de rechten van de mens, de patiëntenverenigingen enzovoort) teneinde erover te waken dat de verwerking van de persoonlijke gezondheidsgegevens het algemeen belang dient en spoort met de algemene verordening gegevensbescherming (AVG), met de waarden van de samenleving en met de redelijke verwachtingen van de burgers, zowel aangaande de bescherming van hun gegevens als aangaande de aanwending van die gegevens voor doeleinden in verband met het beheer van het gezondheidssysteem, met onderzoek, met het opmaken van statistieken of met andere gezondheidsgerelateerde doeleinden die het algemeen belang dienen;

b) een interfederale coördinatie en de bevordering van de samenwerking tussen de zowel openbare als private instellingen die persoonlijke gezondheidsgegevens verwerken, waarbij die coördinatie noodzakelijkerwijze is ingebed in interfederale of nationale plannen inzake volksgezondheidsbeleid[16].

Die samenwerking moet leiden tot het bevorderen van gemeenschappelijke gegevensbestanddelen en -formats, tot het waarborgen van de kwaliteit, alsook tot het uitwerken van normen inzake de operationele compatibiliteit van de gemeenschappelijke gegevens, beleidslijnen en procedures, zodat gegevens op een gecontroleerde en transparantie manier kunnen worden gedeeld voor doeleinden in verband met het beheer van het gezondheidssysteem, met onderzoek, met het opmaken van statistieken of met andere gezondheidsgerelateerde doeleinden die het algemeen belang dienen, en waarbij tegelijk de persoonlijke levenssfeer en de veiligheid van de gegevens worden gewaarborgd;

2. de capaciteiten van de gezondheidsgegevenssystemen die de overheid, met het oog op het dienen en het vrijwaren van het algemeen belang, gebruikt voor de verwerking van de persoonlijke gezondheidsgegevens, te beschrijven, te documenteren en te analyseren. Dat onderzoek zal moeten slaan op:

a) de beschikbaarheid, de kwaliteit, de onderlinge afstemming en de toegankelijkheid van de gegevens, alsmede op de bescherming van de persoonlijke levenssfeer en de veiligheid van de gegevens;

[16] Bijvoorbeeld: kankerplan, verslavingsplan, vaccinatieplan.

b) la description, la documentation des sources et types de données, ainsi que sur les éléments du traitement des données autorisés à des fins de gestion du système de santé, de recherche, de statistique ou d'autres objectifs sanitaires répondant à l'intérêt général, sous réserve de garanties appropriées, en particulier relatives aux transferts d'ensembles de données et à la mise en correspondance des dossiers d'ensembles de données;

3. de s'assurer que la communication des informations concernant les données de santé soit claire et compréhensible pour les citoyennes et citoyens. Ces dispositions, définies par le RGPD, devraient prévoir que:

a) lorsque des données à caractère personnel de santé sont recueillies auprès des personnes physiques, celles-ci recevront, en des termes clairs, précis, concis, facilement compréhensibles et bien lisibles, des informations sur le traitement de leurs données personnelles de santé, y compris sur la possible consultation de ces données par des parties tierces avec, toutefois, formalisation des objectifs (recherches, enquêtes santé-environnement, …) et des modalités, et information quant aux objectifs qui sous-tendent ce traitement, aux avantages qu'il apportera, au fondement juridique sur lequel il repose et à la durée de leur conservation;

b) le principe premier régissant l'accès aux données à caractère personnel de santé est la relation thérapeutique entre un prestataire de soins et le patient. Il doit être établi par un acte proactif du patient dans un cadre où il a reçu toutes les informations sur les données récoltées, sur les modalités de partage de ces données et qu'il y consent expressément.

À cet égard, le consentement déduit implicitement du simple fait que le patient ait communiqué à un médecin les données figurant sur sa carte d'identité ne peut être considéré comme étant un consentement éclairé de sa part;

c) conformément aux articles 32, 33 et 34 du RGPD, l'APD (dans les 72 heures) et les personnes concernées (dans les meilleurs délais) seront averties de toute violation ou autre usage abusif de données personnelles de santé. Lorsqu'il ne sera pas possible d'avertir chaque personne concernée, la notification pourra être faite par le biais d'une communication publique efficace;

4. de s'assurer de l'existence de mécanismes d'expression active et valide du consentement éclairé et des

b) het beschrijven en documenteren van de gegevensbronnen en -types, alsmede op de toegestane bestanddelen van de gegevensverwerking voor doeleinden die verband houden met het beheer van het gezondheidssysteem, met onderzoek, met het opmaken van statistieken of met andere gezondheidsgerelateerde doeleinden die het algemeen belang dienen, onder voorbehoud van passende waarborgen, inzonderheid inzake de overheveling van datasets en de onderlinge afstemming van de datasetmappen;

3. te verzekeren dat de informatie over de gezondheidsgegevens op duidelijke en bevattelijke wijze aan de burgers wordt meegedeeld. Daartoe zou in overeenstemming met de AVG het volgende moeten worden bepaald:

a) wanneer van natuurlijke personen persoonlijke gezondheidsgegevens worden verzameld, krijgen de betrokkenen in duidelijke, precieze, beknopte, makkelijk te begrijpen en heel bevattelijke bewoordingen informatie over de verwerking van hun persoonlijke gezondheidsgegevens, alsook over de eventuele raadpleging van die gegevens door derden, waarbij de doelstellingen en de nadere regels (onderzoek, peilingen naar de omgevingsgezondheid enzovoort) formeel worden vastgelegd; voorts krijgen zij informatie over de doelstellingen die aan die verwerking ten grondslag liggen, de voordelen ervan, de rechtsgrond waarop de verwerking berust en de bewaringstermijn van de gegevens;

b) het belangrijkste beginsel voor de toegang tot de persoonlijke gezondheidsgegevens is de therapeutische relatie tussen een zorgverstrekker en de patiënt. Die moet worden vastgesteld via een proactieve handeling door de patiënt, die inhoudt dat hij volledig is geïnformeerd over de verzamelde gegevens en over de wijze waarop die gegevens worden gedeeld, alsook dat hij daartoe uitdrukkelijk zijn toestemming geeft.

In dat verband kan een impliciete toestemming voortvloeiend uit het loutere feit dat een patiënt een arts de gegevens op zijn identiteitskaart heeft verstrekt, niet worden beschouwd als een geïnformeerde toestemming;

c) overeenkomstig de artikelen 32, 33 en 34 van de AVG moeten de GBA (binnen de 72 uur) en de betrokkenen (zo spoedig mogelijk) op de hoogte worden gebracht van elke schending of elk ander oneigenlijk gebruik van persoonlijke gezondheidsgegevens. Indien niet elke betrokkene op de hoogte kan worden gebracht, mag de melding gebeuren via een doeltreffende publieke communicatie;

4. te zorgen voor regelingen voor de actieve en geldige uiting van de geïnformeerde toestemming, evenals

procédures validant et certifiant que le patient a reçu et compris les informations portant sur les usages non thérapeutiques de ses données personnelles ainsi que sur le degré d'anonymisation et/ou de pseudonymisation de ces données pour d'autres finalités de santé publique. En cas de dérogation au principe de consentement, il s'impose de déterminer précisément les motifs d'incapacité individuelle ou d'urgence impérative sous-tendant la dérogation;

5. de prévoir que, lorsque le traitement des données à caractère personnel de santé est fondé sur le consentement des personnes physiques, celui-ci ne soit valide que s'il est explicite et librement donné et que ces personnes disposant de mécanismes clairs, visibles et faciles à utiliser, puissent, le cas échéant, revenir sur leur consentement portant sur l'utilisation future de leurs données. Lorsque le traitement des données à caractère personnel de santé n'est pas fondé sur le consentement, des mécanismes devront être prévus pour permettre aux personnes physiques d'exprimer préalablement leurs préférences quant au traitement de leurs données de santé, de s'opposer au traitement de telles données dans certaines circonstances ou d'exprimer explicitement s'ils acceptent que leurs données à caractère personnel de santé soient partagées à des fins de recherche publique ou d'autres objectifs de santé conformes à l'intérêt général. Le consentement doit également permettre à la personne d'opérer une distinction claire quant aux types d'acteurs du secteur de la santé (publics, publics et privés ou purement privés), appelés à utiliser ses propres données à caractère personnel de santé pseudonymisées. De même, la personne sera informée de l'anonymisation possible de ses données dans le cadre de traitements ultérieurs;

6. d'assurer et d'organiser la transparence du traitement des données par des mécanismes d'information publique qui ne compromettent pas la confidentialité et la sécurité des données à caractère personnel de santé. L'information publique devra contenir les éléments suivants:

a) les objectifs du traitement des données à caractère personnel de santé, les objectifs sanitaires d'intérêt général poursuivis par ce traitement ainsi que le fondement juridique sur lequel il repose;

b) les informations concernant la mise en œuvre du cadre de gouvernance relatif aux données de santé et son efficacité;

voor procedures ter bekrachtiging en waarborging dat de patiënt de informatie over het niet-therapeutische gebruik van zijn persoonsgegevens en over de mate van anonimisering en/of de pseudonimisering van die gegevens voor andere volksgezondheidsdoeleinden heeft ontvangen en begrepen. Indien van het beginsel van toestemming wordt afgeweken, dient nauwkeurig te worden aangegeven welke redenen van individueel onvermogen of welke dringende noodzaak aan die afwijking ten grondslag liggen;

5. te bepalen dat wanneer de verwerking van de persoonlijke gezondheidsgegevens berust op de toestemming van de natuurlijke personen, die toestemming alleen geldig is indien zij uitdrukkelijk en vrijwillig werd verleend, en dat die personen, voor wie heldere, zichtbare en gebruiksvriendelijke procedures ter beschikking zijn, in voorkomend geval kunnen terugkomen op hun toestemming voor het toekomstige gebruik van hun gegevens. Wanneer de verwerking van de persoonlijke gezondheidsgegevens niet op toestemming berust, moet worden voorzien in regelingen die de natuurlijke personen in staat stellen hun voorkeuren met betrekking tot de verwerking van hun gezondheidsgegevens vooraf kenbaar te maken, bezwaar te maken tegen de verwerking van dergelijke gegevens in bepaalde omstandigheden, dan wel uitdrukkelijk aan te geven of zij ermee instemmen dat hun persoonlijke gezondheidsgegevens worden gedeeld voor openbaar onderzoek of andere gezondheidsgerelateerde doeleinden die stroken met het algemeen belang. De toestemming moet de betrokkene tevens in staat stellen een duidelijk onderscheid te maken tussen de verschillende soorten actoren van de gezondheidssector (publiek, publiek-privé of louter privé) die zijn gepseudonimiseerde persoonlijke gezondheidsgegevens moeten gebruiken. De betrokkene zal bovendien op de hoogte worden gebracht van de eventuele anonimisering van zijn gegevens in het kader van latere verwerkingen;

6. de transparantie van de gegevensverwerking te waarborgen en te organiseren door middel van procedures voor publieke informatieverstrekking die de vertrouwelijkheid en de veiligheid van de persoonlijke gezondheidsgegevens niet in het gedrang brengen. De publieke informatie moet de volgende elementen bevatten:

a) de doelstellingen van de verwerking van de persoonlijke gezondheidsgegevens, de gezondheidsdoelstellingen van algemeen belang die met die verwerking worden nagestreefd en de rechtsgrond waarop die berust;

b) de informatie over de tenuitvoerlegging en de efficiëntie van het raamwerk voor het beheer van de gezondheidsgegevens;

7. de mettre en œuvre des mécanismes de suivi et d'évaluation. Ces mécanismes devront:

a) permettre de déterminer si les usages relatifs aux données à caractère personnel de santé ont répondu aux objectifs sanitaires poursuivis dans l'intérêt de la collectivité et ont apporté les bénéfices attendus, si des usages inappropriés ou des violations et usages abusifs des données sont apparus, entraînant notamment le non-respect de la législation, et prévoir, le cas échéant, des mécanismes de sanction;

b) permettre l'utilisation des résultats de cette évaluation dans le cadre d'un processus d'amélioration continue par un examen régulier de l'évolution de la disponibilité des données à caractère personnel de santé, des besoins de la recherche médicale et des activités connexes ainsi que des besoins de l'action publique;

c) permettre d'évaluer et d'actualiser de manière régulière les politiques et pratiques employées pour gérer les risques relatifs à la vie privée, à la protection des données à caractère personnel de santé et à la sécurité en lien avec la gouvernance de ces données;

d) permettre un contrôle parlementaire régulier, par voie d'auditions et de rapports émanant des organismes de gestion de ces données et des associations de patients, un tel contrôle parlementaire impliquant une évaluation de la gouvernance et des acteurs habilités à traiter les données à caractère personnel de santé;

8. de mettre en place un système de formation et de développement des compétences, organisé par les autorités, en matière de protection de la vie privée et de sécurité à l'intention des acteurs du traitement des données à caractère personnel de santé. L'APD définira le contenu de ces formations et sera responsable de la sélection des organismes de formation habilités à les dispenser;

9. de mettre en place des mesures de contrôle et des garanties qui devront:

a) prévoir un mécanisme d'audit régulier et indépendant visant à contrôler les organismes publics et privés chargés du traitement des données à caractère personnel de santé afin de s'assurer de la légalité des traitements qu'ils effectuent et de la fiabilité des technologies qu'ils utilisent. Cette mission peut être confiée à l'Autorité de protection des données;

7. opvolgings- en evaluatieregelingen uit te werken. Die regelingen moeten het mogelijk maken:

a) vast te stellen of de persoonlijke gezondheidsgegevens werden gebruikt in overeenstemming met de in het belang van de gemeenschap nagestreefde gezondheidsgerelateerde doelstellingen, en of het gebruik ervan de verwachte voordelen heeft opgeleverd, alsook vast te stellen of sprake is geweest van oneigenlijk gebruik, schendingen of misbruik van gegevens, waardoor de wetgeving niet werd nageleefd; in voorkomend geval moeten sanctieregelingen worden ingesteld;

b) de resultaten van die evaluatie te gebruiken in het kader van een permanent verbeteringsproces, door te voorzien in een geregelde analyse van de evolutie van de beschikbaarheid van de persoonlijke gezondheidsgegevens, van de behoeften inzake medisch onderzoek en van de aanverwante activiteiten, alsook van de behoeften inzake strafvordering;

c) het beleid en de praktijken voor het beheer van de risico's voor de persoonlijke levenssfeer, de bescherming van de persoonlijke gezondheidsgegevens en de veiligheid met betrekking tot het beheer van die gegevens regelmatig te evalueren en bij de tijd te brengen;

d) op gezette tijdstippen parlementair toezicht uit te oefenen door middel van hoorzittingen en verslagen van de instanties belast met het beheer van die gegevens en van de patiëntenverenigingen; een dergelijk parlementair toezicht impliceert immers een evaluatie van het bestuur en van de actoren die gemachtigd zijn de persoonlijke gezondheidsgegevens te verwerken;

8. werk te maken van een door de overheid georganiseerd systeem voor opleiding en ontwikkeling van vaardigheden inzake van de persoonlijke levenssfeer en de veiligheid ten behoeve van wie betrokken is bij de verwerking van de persoonlijke gezondheidsgegevens. De GBA zal de inhoud van die opleidingen bepalen en zal verantwoordelijk zijn voor de selectie van de opleidingsinstellingen die gemachtigd zijn voor het verstrekken ervan;

9. toezichtmaatregelen en waarborgen in te stellen die:

a) een regeling omvatten voor een regelmatige en onafhankelijke audit van de overheids- en privéinstanties die belast zijn met de verwerking van de persoonlijke gezondheidsgegevens, teneinde te verzekeren dat zij de gegevens wettig verwerken en de daarbij toegepaste technologieën betrouwbaar zijn. Die opdracht kan aan de Gegevensbeschermingsautoriteit worden toevertrouwd;

b) définir clairement et précisément le statut et les responsabilités du personnel chargé du traitement des données à caractère personnel de santé et de définir les incompatibilités et les conflits d'intérêts;

c) s'assurer concrètement que le traitement des données à caractère personnel de santé puisse uniquement être réalisé par, ou confié à, des organismes prévoyant une formation appropriée en matière de confidentialité et de sécurité des données destinée à l'ensemble de leur personnel et s'assurer sur le terrain qu'une telle formation appropriée est effectivement dispensée. Le contenu de la formation et les organismes qui la dispensent seront agréés par l'Autorité de protection des données;

d) inclure des processus formels d'actualisation annuelle des analyses d'impact telles qu'imposées par les articles 35 et 36 du Règlement général sur la protection des données (RGPD);

10. de mettre en place des mesures technologiques, physiques et organisationnelles conçues pour protéger la vie privée et la sécurité tout en préservant, autant que possible, l'utilité des données personnelles de santé au regard des objectifs sanitaires répondant à l'intérêt général et ce, conformément à l'article 32 du *Règlement général sur la protection des données* (*RGPD*). Ces mesures devraient comprendre les éléments suivants:

a) la mise en place de mécanismes limitant l'identification des personnes physiques, notamment par l'anonymisation de leurs données personnelles de santé et tenant compte de l'usage proposé de ces données;

b) la mise en place de conventions transparentes d'utilisation des données personnelles de santé lorsque celles-ci sont partagées avec des tiers en vue de leur traitement, contribuant à optimiser les avantages et à gérer les risques tout en préservant l'utilité de telles données personnelles. Il convient que ces accords spécifient les arrangements et mécanismes nécessaires conçus pour sécuriser les transferts de données et prévoient des moyens adaptés pour sanctionner le non-respect des dispositions;

c) la mise en place de mécanismes solides et convaincants de vérification et d'authentification de l'identité des personnes ayant accès aux données de santé à caractère personnel;

11. de manière plus large, en matière de gouvernance et de protection des données:

b) duidelijk en nauwgezet de status en de verantwoordelijkheden bepalen van het personeel dat belast is met de verwerking van de persoonlijke gezondheidsgegevens en die tevens de onverenigbaarheden en belangenconflicten bepalen;

c) er concreet voor zorgen dat de verwerking van de persoonlijke gezondheidsgegevens uitsluitend kan worden uitgevoerd door of toevertrouwd aan instanties die hun personeel een passende opleiding inzake vertrouwelijkheid en veiligheid van gegevens aanbieden, en dat een dergelijke opleiding in de praktijk ook daadwerkelijk wordt verstrekt. De inhoud van de opleiding en de instanties die ze verstrekken moeten door de Gegevensbeschermingsautoriteit worden erkend;

d) formele en jaarlijks geactualiseerde effectenbeoordelingen omvatten, zoals opgelegd bij de artikelen 35 en 36 van de algemene verordening gegevensbescherming (AVG);

10. technologische, fysieke en organisatorische maatregelen te nemen om de persoonlijke levenssfeer en de veiligheid te beschermen en er tegelijk voor te zorgen dat de persoonlijke gezondheidsgegevens zo veel mogelijk bruikbaar blijven in het licht van de gezondheidsdoelstellingen van algemeen belang, in overeenstemming met artikel 32 van de algemene verordening gegevensbescherming (AVG). Die maatregelen moeten de volgende aspecten omvatten:

a) het instellen van procedures die de identificatie van natuurlijke personen bemoeilijken, meer bepaald via de anonimisering van hun persoonlijke gezondheidsgegevens en door rekening te houden met het beoogde gebruik van die gegevens;

b) de totstandkoming van transparante conventies voor het gebruik van de persoonlijke gezondheidsgegevens wanneer die voor hun verwerking met derden worden gedeeld, wat moet bijdragen tot de optimalisering van de voordelen en het beheer van de risico's zonder dat dergelijke persoonsgegevens aan bruikbaarheid inboeten. Die overeenkomsten moeten specifiëren welke noodzakelijke afspraken en regelingen werden uitgewerkt om de gegevensoverdracht te beveiligen en moeten in passende middelen voorzien om de niet-naleving van de bepalingen te sanctioneren;

c) de ontwikkeling van degelijke en overtuigende regelingen voor de verificatie en de authenticatie van de identiteit van de personen die toegang hebben tot de persoonlijke gezondheidsgegevens;

11. in ruimere zin en met betrekking tot het beheer en de bescherming van de gegevens:

a) d'établir un cadastre des données à caractère personnel mis à la disposition de l'État ayant pour objectif de répondre à des exigences de transparence à l'égard du citoyen;

b) d'évaluer de manière approfondie l'architecture du paysage belge du traitement des données à caractère personnel et notamment le fonctionnement et les missions du comité de sécurité de l'information (CSI), en modifiant, si nécessaire, la loi du 5 septembre 2018 instituant le comité précité et diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données);

c) de résoudre les problèmes d'indépendance susceptibles de toucher les organes étatiques gérant les bases de données à caractère personnel;

d) de soumettre tout projet concernant l'utilisation de données à caractère personnel dans le cadre de la loi du 11 avril 1994 relative à la publicité de l'administration, à l'avis du Conseil d'État et, le cas échéant, à l'Autorité de protection des données et à l'Institut Fédéral pour la Protection et la Promotion des Droits Humains (IFDH).

22 mars 2021

Laurence HENNUY (Ecolo-Groen)
Barbara CREEMERS (Ecolo-Groen)
Cécile THIBAUT (Ecolo-Groen)
Stefaan VAN HECKE (Ecolo-Groen)
Gilles VANDEN BURRE (Ecolo-Groen)
Marie-Colline LEROY (Ecolo-Groen)
Séverine de LAVELEYE (Ecolo-Groen)
Evita WILLAERT (Ecolo-Groen)
Guillaume DEFOSSÉ (Ecolo-Groen)
Kristof CALVO (Ecolo-Groen)

a) te voorzien in een kadaster van persoonsgegevens ten behoeve van de Staat, teneinde te voldoen aan de vereisten inzake transparantie ten aanzien van de burger;

b) een grondige evaluatie uit te voeren van de architectuur van het Belgische landschap van de verwerking van persoonsgegevens en meer bepaald van de werking en de opdrachten van het Informatieveiligheidscomité (IVC), indien nodig via een wijziging van de wet van 5 september 2018 tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van Verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming);

c) een oplossing uit te werken voor de problemen op het vlak van de onafhankelijkheid waarmee de overheidsorganen die de databanken met persoonsgegevens beheren, kunnen worden geconfronteerd;

d) elk project dat betrekking heeft op het gebruik van persoonsgegevens in het kader van de wet van 11 april 1994 betreffende de openbaarheid van bestuur ter advies voor te leggen aan de Raad van State en, in voorkomend geval, aan de Gegevensbeschermingsautoriteit en aan het Federaal instituut voor de bescherming en de bevordering van de rechten van de mens (FIRM).

22 maart 2021

Imprimerie centrale – Centrale drukkerij