CONSEIL D'ÉTAT
section de législation

avis 63.202/2
du 26 avril 2018

sur

un avant-projet de loi '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 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'

RAAD VAN STATE
afdeling Wetgeving

advies 63.202/2
van 26 april 2018

over

een voorontwerp van wet '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'

‡LW-BGFSMBJEA-GDCACUQ‡

Le 22 mars 2018, le Conseil d'État, section de législation, a été invité par la Ministre des Affaires sociales et de la Santé publique à communiquer un avis, dans un délai de trente jours, sur un avant projet de loi '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 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'.

L'avant-projet a été examiné par la deuxième chambre le 23 avril 2018. La chambre était composée de Pierre VANDERNOOT, président de chambre, Luc DETROUX et Wanda VOGEL, conseillers d'État, Sébastien VAN DROOGHENBROECK et Jacques ENGLEBERT, assesseurs, et Béatrice DRAPIER, greffier.

Le rapport a été présenté par Pauline LAGASSE, auditeur. Élise DEGRAVE, appelée en qualité d'experte sur la base de l'article 82 des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973, a également présenté un rapport.

L'avant-projet a été examiné par la deuxième chambre le 26 avril 2018. La chambre était composée de Pierre VANDERNOOT, président de chambre, Luc DETROUX et Wanda VOGEL, conseillers d'État, et Béatrice DRAPIER, greffier.

Le rapport a été rédigé par Pauline LAGASSE, auditeur. Elise DEGRAVE, appelée en qualité d'experte sur la base de l'article 82 des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973, a également présenté un rapport.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de Pierre VANDERNOOT et Wanda VOGEL.

L'avis, dont le texte suit, a été donné le 26 avril 2018.

*

‡LW-BGFSMBJEA-GDCACUQ‡

Op 22 maart 2018 is de Raad van State, afdeling Wetgeving, door de Minister van Sociale Zaken en Volksgezondheid verzocht binnen een termijn van dertig dagen een advies te verstrekken over een voorontwerp van wet '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'.

Het voorontwerp is door de tweede kamer onderzocht op 23 april 2018. De kamer was samengesteld uit Pierre VANDERNOOT, kamervoorzitter, Luc DETROUX en Wanda VOGEL, staatsraden, Sébastien VAN DROOGHENBROECK en Jacques ENGLEBERT, assessoren, en Béatrice DRAPIER, griffier.

Het verslag is uitgebracht door Pauline LAGASSE, auditeur. Élise DEGRAVE, die als expert opgeroepen is op grond van artikel 82 van de wetten 'op de Raad van State', gecoördineerde op 12 januari 1973, heeft eveneens verslag uitgebracht.

Het voorontwerp is door de tweede kamer onderzocht op 26 april 2018. De kamer was samengesteld uit Pierre VANDERNOOT, kamervoorzitter, Luc DETROUX en Wanda VOGEL, staatsraden, en Béatrice DRAPIER, griffier.

Het verslag is opgesteld door Pauline LAGASSE, auditeur. Elise DEGRAVE, die als expert opgeroepen is op grond van artikel 82 van de wetten 'op de Raad van State', gecoördineerde op 12 januari 1973, heeft eveneens verslag uitgebracht.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Pierre VANDERNOOT en Wanda VOGEL.

Het advies, waarvan de tekst hierna volgt, is gegeven op 26 april 2018.

*

‡LW-BGFSMBJEA-GDCACUQ‡

Comme la demande d'avis est introduite sur la base de l'article 84, § 1er, alinéa 1er, 2°, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973, la section de législation limite son examen au fondement juridique de l'avant-projet ‡, à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

Sur ces trois points, l'avant-projet appelle les observations suivantes.

OBSERVATIONS GÉNÉRALES

A. Le droit au respect de la vie privée

1. Comme l'a encore récemment rappelé la Cour constitutionnelle [1], s'agissant du droit au respect de la vie privée garanti par l'article 22 de la Constitution, combiné avec l'article 8 de la Convention européenne des droits de l'homme, l'article 17 du Pacte international relatif aux droits civils et politiques et les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, la portée de l'article 8 de la Convention est analogue à celle de la disposition constitutionnelle précitée, de sorte que les garanties que fournissent ces deux dispositions forment un ensemble indissociable.

Les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne ont, en ce qui concerne le traitement des données à caractère personnel dans le cadre de la mise en œuvre du droit de l'Union, une portée analogue à celle de l'article 8 de la Convention européenne des droits de l'homme et de l'article 22 de la Constitution. Il en va de même de l'article 17 du Pacte international relatif aux droits civils et politiques.

Le droit au respect de la vie privée, tel qu'il est garanti par les dispositions constitutionnelles et conventionnelles précitées, a pour but essentiel de protéger les personnes contre les ingérences dans leur vie privée. Ce droit a une portée étendue et englobe notamment la protection des données à caractère personnel et des informations personnelles.

À cet égard et en ce qui concerne les domaines d'application en dehors de l'Union européenne, la Convention n° 108 du Conseil de l'Europe 'pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel', qui lie l'État belge, impose également une série de garanties minimales à l'État belge.

2.1. Ce droit n'est cependant pas absolu. Il n'exclut pas toute ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée mais il est requis qu'elle soit prévue par une disposition législative suffisamment précise, qu'elle réponde à un besoin social impérieux dans une société démocratique et qu'elle soit proportionnée à l'objectif légitime qu'elle poursuit. Ces dispositions engendrent de surcroît l'obligation positive, pour l'autorité publique, de prendre des mesures qui assurent le respect effectif de la vie privée, même dans la sphère des relations entre les individus.

‡ S'agissant d'un avant-projet de loi, on entend par « fondement juridique » la conformité aux normes supérieures.

[1] C.C., 14 juillet 2016, n° 108/2016, B.7 à B.13 ; 15 mars 2018, n° 29/2018, B.9 à B.15.

‡LW-BGFSMBJEA-GDCACUQ‡

2.2. En réservant au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée, l'article 22 de la Constitution garantit à tout citoyen qu'aucune ingérence dans l'exercice de ce droit ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue. Une délégation à un autre pouvoir n'est toutefois pas contraire au principe de légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur.

À cet égard, la Cour constitutionnelle et la section de législation du Conseil d'État ont plusieurs fois souligné que le débat démocratique est une garantie pour la protection de la vie privée des citoyens. Ainsi affirment-elles qu'

> « en plaçant la protection de la vie privée sous la sauvegarde de la loi elle-même, le Constituant a entendu que les cas et conditions dans lesquels il pourrait y être porté atteinte soient soumis à la décision d'assemblées délibérantes démocratiquement élues » [2].

L'intervention des parlementaires doit être assurée car

> « c'est précisément là où les risques pour la protection de la vie privée sont les plus grands, que le législateur doit être associé de la manière la plus directe qui soit à la confection des normes » [3].

Si cette tâche n'était pas assumée par le pouvoir législatif, cela reviendrait

> « pour le législateur, désigné par la Constitution comme le gardien du respect du droit au respect de la vie privée, [à renoncer] à définir lui-même quelles sont les intrusions qui peuvent venir restreindre le droit dont il a la garde. L'article 22 de la Constitution lui interdit de faire ce choix » [4].

2.3. Outre l'exigence de légalité formelle, l'article 22 de la Constitution impose également que l'ingérence dans l'exercice du droit au respect de la vie privée soit définie en des termes clairs et suffisamment précis qui permettent d'appréhender de manière prévisible les hypothèses dans lesquelles le législateur autorise une pareille ingérence.

De même, l'exigence de prévisibilité à laquelle la loi doit satisfaire pour être jugée conforme à l'article 8 de la Convention européenne des droits de l'homme implique que sa formulation soit assez précise pour que chacun puisse – en s'entourant au besoin de conseils

---

[2] Avis n° 37.765/1/2/3/4 donné le 4 novembre 2004 sur un avant-projet devenu la loi-programme du 27 décembre 2004, *Doc. parl.*, Chambre, 2004-2005, n° 1437/2 ; avis n[os] 37.748/AG et 37.749/AG donnés le 23 novembre 2004 sur un avant-projet devenu la loi du 3 mai 2005 'modifiant la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité' (37.748/AG) et sur un avant-projet devenu la loi du 3 mai 2005 'modifiant la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitation de sécurité' (37.749/AG), *Doc. parl.*, Chambre, 2004-2005, n[os] 1598/1 et 1599/1 ; C.C., 21 décembre 2004, n° 202/2004, B.4.3 et B.6.3 ; 26 juin 2008, n° 95/2008, B.42 ; 18 mars 2010, n° 29/2010, B.16.1 ; 14 février 2013, n° 6/2013, B.5.7 ; 16 mai 2013, n° 66/2013, B.11.1.

[3] Avis n° 33.487/1/3 des 18 et 20 juin 2002 sur un avant-projet devenu la loi du 22 août 2002 'portant des mesures en matière de soins de santé', *Doc. parl.*, Chambre, 2002-2003, n° 2125/2, p. 539.

[4] Avis n° 26.198/2 donné le 2 février 1998 sur un avant-projet devenu la loi du 11 décembre 1998 'transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil 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', *Doc. parl.*, Chambre, 1997-1998, n° 49-1566/1, p. 201.

‡LW-BGFSMBJEA-GDCACUQ‡

éclairés – prévoir, à un degré raisonnable, dans les circonstances de la cause, les conséquences d'un acte déterminé. La législation doit donner à chacun une indication suffisante sur les circonstances dans lesquelles et à quelles conditions elle habilite la puissance publique à recourir à des mesures affectant les droits protégés par la Convention. Plus particulièrement, lorsque l'intervention de l'autorité présente un caractère secret, la loi doit offrir des garanties suffisantes contre les ingérences arbitraires dans l'exercice du droit au respect de la vie privée, en délimitant le pouvoir d'appréciation des autorités concernées avec une netteté suffisante, d'une part, et en prévoyant des procédures qui permettent un contrôle effectif, d'autre part.

Il découle dès lors de l'article 8 de la Convention et de l'article 22 de la Constitution qu'il doit être prévu de manière suffisamment précise dans quelles circonstances un traitement de données à caractère personnel est autorisé. Le niveau requis de précision de la législation concernée – laquelle ne peut du reste parer à toute éventualité – dépend notamment, selon la Cour européenne des droits de l'homme, du domaine qu'elle est censée couvrir et du nombre et de la qualité de ses destinataires. Ainsi, cette Cour a jugé que l'exigence de prévisibilité dans des domaines liés à la sécurité nationale ne pouvait avoir la même portée que dans d'autres domaines [5].

2.4. Une ingérence des pouvoirs publics dans l'exercice du droit au respect de la vie privée doit non seulement reposer sur une disposition législative suffisamment précise mais aussi reposer sur une justification raisonnable et être proportionnée aux buts poursuivis par le législateur, qui dispose en la matière d'une marge d'appréciation. Cette marge n'est toutefois pas illimitée : pour qu'une norme soit compatible avec le droit au respect de la vie privée, il faut que le législateur ait établi un juste équilibre entre tous les droits et intérêts en cause.

En ce qui concerne la proportionnalité, la Cour européenne des droits de l'homme et la Cour de justice de l'Union européenne tiennent compte de l'existence ou non, dans la réglementation visée, des garanties matérielles et procédurales. Pour juger du caractère proportionné de mesures relatives au traitement de données à caractère personnel, il convient de tenir compte notamment de leur caractère automatisé, des techniques utilisées, de la précision, de la pertinence et du caractère excessif ou non des données traitées, de l'existence ou de l'absence de mesures qui limitent la durée de conservation des données, de l'existence ou de l'absence d'un système de contrôle indépendant permettant de vérifier si la conservation des données est encore requise, de la présence ou de l'absence de droits de contrôle et de voies de recours suffisants pour les personnes concernées, de la présence ou de l'absence de garanties visant à éviter la stigmatisation des personnes dont les données sont traitées, du caractère distinctif de la réglementation et de la présence ou de l'absence de garanties visant à éviter l'usage inapproprié et abusif, par les services publics, des données à caractère personnel traitées.

3. En l'espèce, le droit au respect de la vie privée est au cœur de l'avant-projet soumis à la section de législation. C'est donc au regard des principes qui viennent d'être rappelés que l'avant-projet a été examiné.

[5] Cour eur. D.H., arrêt *Leander c. Suède*, 26 mars 1987, § 51; arrêt *Lupsa c. Roumanie*, 4 juillet 2006, § 33.

‡LW-BGFSMBJEA-GDCACUQ‡

B. La conception générale de la législation relative aux traitements de données à caractère personnel dans l'administration

1. Il est compréhensible que tant l'autorité fédérale que les entités fédérées estiment nécessaire d'adopter des législations spécifiques pour encadrer certains types de traitements de données. Ainsi, au niveau fédéral, des législations sectorielles, telles que la loi du 8 août 1983 'organisant un registre national des personnes physiques', la loi du 15 janvier 1990 'relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale' et la loi du 19 mai 2010 'portant création de la Banque-Carrefour des véhicules', encadrent depuis plusieurs années les traitements de données spécifiques dans des secteurs particuliers de l'administration.

Néanmoins, bien qu'ayant leurs particularités, ces secteurs de l'administration rencontrent aussi des préoccupations communes, à commencer par l'efficacité administrative dans le respect de la protection de la vie privée des citoyens, et des points communs, comme les outils utilisés pour réaliser les traitements de données concernés (sources authentiques de données, intégrateurs de services, identifiants, etc.). En ce sens, l'avant-projet de loi qui a fait l'objet, le 19 avril 2018, de l'avis n° 63.192/2 du Conseil d'État, qui tend à établir la loi-cadre de mise en œuvre du règlement 2016/679/UE 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' (ci-après : « la loi-cadre »), consacre une section particulière au secteur public, avec des concepts et des règles communs [6].

La question de l'échange des données entre administrations est un des éléments communs aux différents secteurs de l'administration. Elle est d'ailleurs abordée par l'avant-projet de loi-cadre évoqué ci-dessus, qui organise l'échange des données via une règle commune pour le secteur public et de protocoles d'échanges entre responsables de traitement des données à caractère personnel.

Or, l'avant-projet s'écarte de cette règle commune et crée une autorité semblable à ce qui est encore aujourd'hui les comités sectoriels supprimés par la loi du 3 décembre 2017 'portant création de l'Autorité de protection des données', qui entrera en vigueur pour l'essentiel le 25 mai 2018. Ni le texte de l'avant-projet ni l'exposé des motifs de la loi-cadre ne justifient la mise en place d'un contrôle distinct de celui organisé par celle-ci ni la nécessité de faire renaître un comité sectoriel.

L'articulation entre l'avant-projet de loi-cadre et le présent avant-projet gagnerait à être réexaminée au regard de ces constats.

2. Par ailleurs, le type de contrôle créé par l'avant-projet manque de cohérence par rapport à celui que l'avant-projet de loi-cadre organise pour les traitements de données effectués dans le secteur public.

En particulier, il est étonnant, dans le chef d'un même législateur, de vouloir, à l'occasion de la régulation des échanges de données entre administrations, tout à la fois

[6] Dans la suite du présent avis, lorsqu'il est question de la loi-cadre, c'est en fonction du contenu de celle-ci, telle qu'elle a été soumise à l'état d'avant-projet à la section de législation, que les observations sont formulées.

‡LW-BGFSMBJEA-GDCACUQ‡

responsabiliser les responsables de traitement du secteur public dans une loi, et les déresponsabiliser dans une autre. En effet, dans la loi-cadre actuellement en projet, plus particulièrement dans la section spécifique consacrée au secteur public (article 22), les responsables de traitement de données sont responsabilisés en leur permettant de conclure entre eux des protocoles d'échanges de données avec l'aide de leur délégué à la protection des données, alors que le présent avant-projet déresponsabilise les responsables de traitement de données puisqu'il institue un organe de contrôle *a priori*, qui, dans les cas visés à l'article 15, § 1er, en projet, de la loi du 15 janvier 1990 (article 19 de l'avant-projet) et l'article 35/1, § 1er, alinéa 3, en projet de la loi du 15 août 2012 'relative à la création et à l'organisation d'un intégrateur de services fédéral' (article 80 de l'avant-projet), autorise ou refuse l'échange de données en amont, à la place des responsables de traitement. La déresponsabilisation des responsables de traitement se marque également au niveau de l'engagement et du fonctionnement du délégué à la protection des données, censé être engagé par le responsable de traitement et exercer ensuite ses fonctions de manière indépendante puisque, dans le présent avant-projet, selon le commentaire de l'article 40, « [l]e comité de sécurité de l'information intervient aussi lors de la désignation et du suivi des délégués à la protection de données […] [pour] vérifier si [la personne concernée] est en mesure d'exercer correctement sa fonction (par exemple en ce qui concerne le temps disponible) et si elle se voit offrir le soutien nécessaire (par exemple sur le plan de la formation) » [7].

Ces difficultés présentent d'autant plus d'acuité que, pour un domaine d'application aussi large, couvrant en effet l'ensemble des services publics fédéraux, la matière sera réglée de manière différente dans deux ensembles de législations distincts, à savoir, d'une part, la loi-cadre et, d'autre part, les lois modifiées par l'avant-projet à l'examen.

Ces deux approches radicalement différentes entre deux avant-projets que le Gouvernement entend déposer simultanément devant le Parlement non seulement traduisent un manque de vision globale mais incitent également à sérieusement douter du respect du principe d'égalité dans la protection du droit à la protection de la vie privée.

C. Le caractère lacunaire de l'avant-projet

L'avant-projet ressuscite le comité sectoriel de la sécurité sociale et de la santé, qui a été supprimé par la loi du 3 décembre 2017 'portant création de l'Autorité de protection des données', en créant le comité de sécurité de l'information.

[7] Voir l'article 46, § 1er, 8°, en projet de la loi du 15 janvier 1990 (article 40 de l'avant-projet).

‡LW-BGFSMBJEA-GDCACUQ‡

L'intention de l'auteur de l'avant-projet est d'habiliter le comité à prendre des décisions administratives (autoriser ou refuser un échange de données) [8]. Si le chapitre 2 instituant le comité contient des règles relatives à la composition de ce comité, il y a lieu de compléter l'avant-projet par des dispositions qui délimitent la compétence de la chambre « autorité fédérale » de manière claire et cohérente, en particulier quant aux critères qui, s'ils sont remplis, rendent nécessaire une décision de ce comité [9].

Par ailleurs, on s'interroge sur les objectifs poursuivis par cet organe de contrôle. Les données de sécurité sociale et les données de santé circulent au sein de deux réseaux sectoriels distincts, ayant en leur cœur deux intégrateurs de services distincts (la Banque-Carrefour de la sécurité sociale pour le réseau de la sécurité sociale et la Plate-forme *eHealth* pour le réseau santé). C'est une excellente solution au regard de l'impératif de *Privacy by design* consacré par 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' (ci-après : « le RGPD »). En effet, de cette manière, l'architecture de l'administration est telle qu'elle sépare les données distinctes, utilisées pour des finalités différentes et le risque est écarté de rassembler des données distinctes en un seul lieu, solution qui présenterait davantage de danger pour la protection de la vie privée. Soumettre les données de sécurité sociale et les données de santé au même organe de contrôle et à la même chambre au sein de celle-ci semble nuire à l'impératif de *Privacy by design*. L'avant-projet ne justifie pourtant pas ce choix.

Toujours s'agissant des objectifs de ce contrôle, s'agit-il uniquement de contrôler l'utilisation des données visées ou également le fonctionnement des institutions de sécurité sociale et de santé ? Il est surprenant de constater que l'article 46, § 1er, 7° et 8°, en projet de la loi du 15 janvier 1990 (article 40 de l'avant-projet) confie au comité le soin d'intervenir dans la désignation du délégué à la protection des données de la Banque-Carrefour et de son suivi, et de vérifier si les délégués à la protection des données sont en mesure d'exercer correctement leur fonction, avec le soutien nécessaire.

Enfin, le commentaire de l'article 46 en projet de la loi du 15 janvier 1990 (article 40 de l'avant-projet) expose que les décisions du comité sont contraignantes à l'égard des tiers, peuvent faire l'objet d'un recours au Conseil d'État et sont publiées. Le dispositif ne mentionne pourtant pas d'indication au sujet de la publication des décisions du comité.

Ces importantes lacunes, de même que celles dont il sera fait état dans les observations particulières, doivent être comblées.

D. Le statut du comité de sécurité de l'information

1. Le statut du comité de sécurité de l'information n'apparaît pas clairement et suscite des questions tant au regard de la Constitution qu'au regard du RGPD.

[8] Il est également renvoyé sur ce point à l'observation formulée sous l'article 40.

[9] S'agissant de la chambre « sécurité sociale et santé », ses compétences sont fixées par l'article 46 en projet de la loi du 15 janvier 1990 (article 40 de l'avant-projet).

‡LW-BGFSMBJEA-GDCACUQ‡

2. Il résulte de l'exposé des motifs et de plusieurs dispositions de l'avant-projet que ce comité et les deux chambres qui le composent ont vocation à succéder et à « reprendre les compétences » du comité sectoriel de la sécurité sociale et de la santé, d'une part, et du comité sectoriel pour l'autorité fédérale, d'autre part, tous deux institués au sein de la Commission de la protection de la vie privée [10].

Contrairement à ces deux comités sectoriels, le comité de sécurité de l'information ne sera pas institué au sein de l'Autorité de protection des données, appelée à succéder à la Commission de la protection de la vie privée en vertu de la loi du 3 décembre 2017 'portant création de l'Autorité de protection des données'. L'exposé des motifs confirme en outre que l'intention de l'auteur de l'avant-projet n'est pas de faire de ce comité une « autorité de contrôle » au sens du RGPD, à savoir une « autorité publique indépendante qui est instituée par un État membre » et qui est « chargée […] de surveiller l'application du présent règlement, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union » [11].

Plusieurs dispositions de l'avant-projet traduisent la volonté de son auteur de faire de ce comité une autorité administrative indépendante pouvant, notamment, autoriser différents traitements des données à caractère personnel effectués par les services publics, voire, dans certaines hypothèses, fixer des règles à suivre pour ces traitements [12].

Si le comité est appelé à prendre de telles décisions et s'il n'est pas lui-même une autorité de contrôle au sens du RGPD, il apparaît devoir être considéré, au regard de celui-ci, comme un « responsable du traitement ».

Un « responsable du traitement » est en effet défini par l'article 4, point 7, du RGPD comme étant

> « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ».

Puisque certaines « délibérations » à prendre par le comité tendent à déterminer les finalités et les moyens de traitement des données traitées par les services publics et si ce comité n'est pas lui-même une autorité de contrôle, il doit donc être soumis à une « autorité de contrôle ». En effet, si le RGPD autorise certaines dérogations pour les missions d'intérêt public [13], il n'autorise pas que des responsables de traitement [14] échappent à la compétence d'une autorité de contrôle.

[10] Article 37 de la loi du 15 janvier 1990 et article 36*bis* de la loi du 8 décembre 1992 'relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel'.

[11] Articles 4, point 21, et 51, paragraphe 1, du RGPD.

[12] Voir not. l'article 40 et, dans le présent avis, l'observation particulière formulée sous cette disposition.

[13] Article 23 du RGPD.

‡LW-BGFSMBJEA-GDCACUQ‡

3. Il résulte de plusieurs dispositions de l'avant-projet que ce comité sera habilité à prendre des décisions « ayant une portée générale contraignante envers les tiers » [15]. Compte tenu de l'imprécision des normes que ce comité devra mettre en œuvre pour prendre celles de ces décisions qu'elles estiment être contraires aux normes supérieures, il jouira d'un large pouvoir discrétionnaire. Or, dans l'exercice de ce pouvoir, ce comité ne sera soumis à aucun contrôle hiérarchique et de tutelle de la part du pouvoir exécutif. Il est même expressément stipulé que les membres de ce comité ne peuvent recevoir d'instructions de personne [16].

Les personnes, et notamment celles dont le traitement des données personnelles sera autorisé par le comité, seront donc liées par ces décisions. Si elles ne sont pas privées d'un recours juridictionnel contre celles de ses décisions qu'elles estiment être contraires aux normes supérieures, elles sont en revanche privées de la garantie de voir les décisions qui les concernent prises par une autorité politiquement responsable.

Tant la section de législation que la Cour constitutionnelle ont certes déjà admis la création d'autorités administratives indépendantes, notamment lorsqu'une réglementation européenne impose la création de telles autorités [17]. En l'occurrence toutefois, le RGPD impose l'indépendance de l'autorité de contrôle et non celle des autorités publiques qui, ne recevant pas le statut d'une telle autorité de contrôle, traitent des données personnelles ou autorisent de tels traitements et doivent précisément être soumises au contrôle de l'autorité de contrôle. En habilitant le comité à prendre des décisions en matière de traitement des données à caractère personnel qui lient les tiers, sans que l'opportunité de telles décisions, même à les supposer conformes aux normes supérieures, ne puisse être soumise au contrôle d'une autorité politiquement responsable, l'avant-projet prive les personnes concernées de la garantie d'un tel contrôle, sans que cela soit justifié par une exigence d'une norme supérieure, telle une norme européenne.

Dès lors, de deux choses l'une :

– soit le comité de sécurité et de l'information est institué en tant qu'autorité de contrôle au sens du RGPD (ou est intégré à l'Autorité de protection des données), moyennant, le cas échéant, une adaptation de ses missions et un renforcement de son indépendance [18] ;

– soit les compétences prévues par la loi en projet lui sont maintenues en tant qu'organe intervenant dans les décisions prises par les services publics de traiter des données

[14] À l'exception des opérations de traitement effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle (article 55 du RGPD).

[15] Article 46, § 2, en projet de la loi du 15 janvier 1990 (article 40 de l'avant-projet).

[16] Article 5 de l'avant-projet.

[17] Voir not. l'avis n° 50.003/4 donné le 26 septembre 2011 sur un avant-projet devenu la loi du 10 juillet 2012 'portant des dispositions diverses en matière de communications électroniques', *Doc. parl.*, Chambre, 2011-2012, n° 53-2143/1, pp.169 à 234, et la jurisprudence de la Cour constitutionnelle à laquelle cet avis se réfère.

[18] L'article 3, notamment, n'interdit pas que les membres de la chambre sécurité sociale et santé du comité relèvent du pouvoir hiérarchique d'un autre ministre que ceux ayant la sécurité sociale ou la santé dans ses attributions. L'article 42 en projet de la loi du 15 janvier 1990 (article 35 de l'avant-projet) fait intervenir les administrations concernées dans la préparation des délibérations à rendre par le comité, ce qui ne serait pas conforme à l'article 52, paragraphe 5, du RGPD, relatif à l'indépendance de l'autorité de contrôle.

‡LW-BGFSMBJEA-GDCACUQ‡

personnelles, auquel cas il ne se justifie pas de ne pas les soumettre tant au contrôle hiérarchique ou de tutelle du pouvoir exécutif [19] que de l'Autorité de protection des données ou d'une autre autorité de contrôle qui serait instituée dans le respect du chapitre VI du RGPD.

*

Ces observations générales tendent à inviter le législateur à concevoir dès à présent, de manière aussi homogène et harmonisée que possible, l'architecture globale de la législation qui, au départ de la loi-cadre et par la succession de lois particulières, formera, en combinaison avec le RGPD, le droit applicable au traitement des données par le secteur public fédéral, dont l'avant-projet à l'examen serait le premier élément faisant suite à l'adoption de la loi-cadre (observation générale B).

Elles contiennent également le constat de graves lacunes dans l'avant-projet (observation générale C).

Elles posent enfin la question du statut du comité de sécurité de l'information et de son articulation avec les compétences de l'Autorité de protection des données (observation générale D).

C'est sous la réserve de ces observations générales que le présent avis est donné.

OBSERVATIONS PARTICULIÈRES

DISPOSITIF

Chapitre 2 – Institution du comite de sécurité de l'information

Dès lors que les compétences du « Comité de sécurité de l'information » ne se réduisent pas à la sécurité de l'information mais consistent à contrôler le respect des règles de protection des données dans leur ensemble, sa dénomination devrait être revue.

Article 10

L'article 10 organise la fusion entre deux fonctions : d'une part, le conseiller en sécurité et, d'autre part, le délégué à la protection des données.

Il s'agit pourtant de deux fonctions distinctes auxquelles correspondent des profils de fonction distincts, contrairement à ce qu'est énoncé dans l'exposé des motifs lorsqu'il indique que le conseiller en sécurité est l'« ancien concept », et que le délégué à la protection des données est le « nouveau concept ».

[19] L'avant-projet est muet sur ce point.

‡LW-BGFSMBJEA-GDCACUQ‡

Le conseiller en sécurité est une fonction créée par la loi du 15 janvier 1990 pour les institutions de sécurité sociale. Elle est décrite à l'article 25 de cette loi, qui dispose ce qui suit :

> « Le Conseiller en sécurité visé à l'article 24, alinéas 1er et 2, assure, pour concourir à la sécurité des données sociales traitées ou échangées par son institution et à la protection de la vie privée des personnes auxquelles ces données sociales ont trait :
>
> 1° la fourniture d'avis qualifiés à la personne chargée de la gestion journalière ;
>
> 2° l'exécution de missions qui lui sont confiées par la personne chargée de la gestion journalière.
>
> Le conseiller en sécurité de la Banque-Carrefour fournit en outre des avis qualifiés relatifs à la sécurité du réseau.
>
> Le Roi peut fixer les règles selon lesquelles le conseiller en sécurité exerce ses missions ».

Le conseiller en sécurité exerce donc, principalement, une fonction dédiée à la sécurité informatique.

Le délégué à la protection des données est une fonction instituée par le RGPD, en ses articles 37 et suivants. Cette fonction est dédiée à la protection des données dans son ensemble, mission plus large que la seule sécurité informatique. Le RGPD mentionne d'ailleurs en son article 37, paragraphe 5, que le délégué à la protection des données est désigné en particulier sur la base de « ses connaissances spécialisées du droit et des pratiques en matière de protection des données ».

La fusion de ces deux fonctions pose question au regard du RGPD, s'agissant tout d'abord de son article 39, qui définit les nombreuses missions du délégué à la protection des données, et de l'article 38, paragraphe 2, qui impose au responsable du traitement de fournir au délégué à la protection des données les « ressources nécessaires pour exercer ses missions », ce qui comprend le temps nécessaire pour se consacrer à ces missions. La fusion de la fonction de conseiller en sécurité et de délégué à la protection des données dans le chef d'une seule personne risque de porter atteinte à ces impératifs.

L'article 10, de même que l'article 49, a) seront réexaminés à la lumière de la présente observation.

Article 12

1. L'article 5*bis* en projet de la loi du 15 janvier 1990 habilite certaines administrations, « soit pour ce qui les concerne respectivement, soit en commun, en exécution de leurs missions légales respectives […] », à « recueillir des données à caractère personnel, les traiter et les agréger en vue de la création d'un '*datawarehouse*' leur permettant, d'une part, d'effectuer des contrôles ciblés sur la base d'indicateurs de risques et, d'autre part, de réaliser des analyses sur des données relationnelles en provenance de différentes instances ».

‡LW-BGFSMBJEA-GDCACUQ‡

La section de législation comprend par là que de multiples traitements de données sont créés par cette disposition : la création d'un « *datawarehouse* », la collecte de données (indéterminées dans le texte) par les institutions visées, l'injection de ces données et leur agrégation dans ledit « *datawarehouse* », l'application sur les données stockées dans le « *datawarehouse* » d'algorithmes « anti-fraude », l'application d'une technique de profilage permettant de faire la relation entre les données traitées et des indicateurs de risques de fraude, l'utilisation de ces données dans la prise d'une décision administrative consistant à contrôler les personnes concernées et, par ailleurs, l'utilisation de ces données dans le cadre d'analyse.

Cette disposition appelle les critiques suivantes au regard de l'article 8 de la Convention européenne des droits de l'homme et de l'article 22 de la Constitution, en particulier de l'exigence de légalité et de l'exigence de prévisibilité qu'ils comportent, ainsi que des articles 6, paragraphe 3, et 22 du RGPD.

L'exigence de légalité impose notamment de confier au législateur la détermination des conditions d'admissibilité du traitement des données à caractère personnel, et non à l'administration elle-même : si l'organisation de traitements de données était laissée à la discrétion des administrations, celles-ci pourraient avoir tendance à apprécier la nécessité de tels traitements principalement au regard de leur intérêt immédiat, celui de l'efficacité administrative, et à donner trop peu de poids à la protection de la vie privée des citoyens.

2. L'article 22 de la Constitution impose également au législateur d'adopter une loi qui soit accessible et compréhensible [20], exigence reprise dans la jurisprudence de la Cour constitutionnelle comme rappelé ci-avant.

Outre le fait qu'une telle clarté doit permettre à tout individu de connaître les conséquences que la loi réserve à ses actes, la précision de la loi est particulièrement importante en matière d'e-gouvernement, dans le souci d'encadrer l'action du pouvoir exécutif et de prévenir et de contrôler les abus de pouvoir. C'est pourquoi toute personne doit connaître « l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré » [21].

Concrètement, comme l'a rappelé l'avis de la Commission de la protection de la vie privée [22], le législateur doit déterminer les éléments essentiels des traitements de données à caractère personnel organisés, ainsi que cela résulte de la jurisprudence de la Cour constitutionnelle et de la section de législation du Conseil d'État.

[20] Voir not. Cour eur. D.H., arrêt *Malone c. Royaume-Uni*, 2 août 1984, § 67. Ces garanties ont été appliquées aux traitements de données dans l'arrêt *Rotaru c. Roumanie* du 4 mai 2000, §§ 52 et 55, de la Cour européenne des droits de l'homme.

[21] Voir not. Cour. eur. D.H., arrêt *Amann c. Suisse*, 16 février 2000, § 62.

[22] Avis n° 34/2018 du 11 avril 2018 sur l'avant-projet faisant l'objet du présent avis. Lorsque, dans le présent avis, il est fait référence à l'avis de la Commission de la protection de la vie privée, c'est à cet avis n° 34/2018 que cette référence est faite.

‡LW-BGFSMBJEA-GDCACUQ‡

En particulier, pour chaque traitement de données, le législateur doit définir lui-même les catégories de données utilisées et leur mode de collecte [23].

L'objectif poursuivi par le traitement, appelé également « finalité » du traitement, est un élément essentiel de celui-ci [24].

Il en va de même de la durée de conservation des données. Cela suppose que le législateur fixe au moins les délais maximums de conservation des données [25].

Le législateur doit déterminer également le responsable du traitement [26].

La communication des informations, dite aussi « réutilisation » doit également être organisée par le législateur lui-même [27].

---

[23] Avis n° 37.765/1/2/3/4 donné le 4 novembre 2004 sur un avant-projet devenu la loi-programme du 27 décembre 2004, *Doc. parl.*, Chambre, 2004-2005, n° 1437, p. 634 ; avis n° 41.662/1/2/3/4 donné les 14, 16 et 17 novembre 2006 sur un avant-projet de loi devenu la loi-programme (I) du 27 décembre 2006, *Doc. parl.*, Chambre, 2006-2007, n° 2773/1, p. 425 ; avis n° 40.079/2 donné le 12 avril 2006 sur un avant-projet devenu la loi du 28 décembre 2006 'portant assentiment au Traité entre le Royaume de Belgique, la République fédérale d'Allemagne, le Royaume d'Espagne, la République française, le Grand-Duché de Luxembourg, le Royaume des Pays-Bas et la République d'Autriche relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale, et aux annexes, faits à Prüm le 27 mai 2005', *Doc. parl.*, Chambre, 2005-2006, n° 2645/1 ; avis n° 27.289/4 donné le 25 février 1998 sur un avant-projet devenu la loi du 21 décembre 1998 'relative à la sécurité lors des matches de football', *Doc. parl.*, Chambre, 1997-1998, n° 1572/1, p. 50 ; avis n^os^ 42.774/3 et 42.775/3 donné le 24 avril 2007 sur un projet d'arrêté royal devenu la loi du 21 août 2008 'relative à l'institution et à l'organisation de la place-forme (lire : plate-forme) eHealth' (42.774/3) et un projet d'arrêté royal devenu la loi du 21 août 2008 (nouvel intitulé) 'relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions' (42.775/3); avis n° 47.162/4 donné le 2 décembre 2009 sur un avant-projet devenu la loi du 19 mai 2010 'portant création de la Banque-Carrefour des véhicules', *Doc. parl.*, Chambre, 2009-2010, n° 52-2493/1, pp. 38 à 48.

[24] C.C., 14 février 2008, n° 15/2008, B.22 ; 18 mars 2010, n° 29/2010, B.11 et s. ; 13 janvier 2011, n° 1/2011, B.12.1 et s. ; avis n° 41.662/1/2/3/4 donné les 14, 16 et 17 novembre 2006 sur un avant-projet devenu la loi-programme (I) du 27 décembre 2006, *Doc. parl.*, Chambre, 2006-2007, n° 2773/1, p. 425 ; avis n° 38.782/2/V donné le 11 août 2005 sur un avant-projet devenu la loi du 10 juillet 2006 'relative à l'analyse de la menace', *Doc. parl.*, Chambre, 2005-2006, n° 2032/1, p. 64.

[25] Avis n^os^ 37.748 et 37.749/AG donnés le 23 novembre 2004 sur un avant-projet devenu la loi du 3 mai 2005 'modifiant la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité' (37.748/AG) et sur un avant-projet devenu la loi du 3 mai 2005 'modifiant la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitation de sécurité' (37.749/AG), *Doc. parl.*, Chambre, 2004-2005, n^os^ 1598/1 et 1599/1.

[26] Commission de la protection de la vie privée, avis n° 23/2008 du 11 juin 2008 relatif à un avant-projet de loi 'portant création de la source authentique des données relatives aux véhicules', n° 49 ; avis n° 42/2006 donné le 18 octobre 2006 concernant l'avant-projet de loi portant création d'une source authentique relatives aux véhicules, n° 11.

[27] Avis n° 27.289/4 donné le 25 février 1998 sur un avant-projet devenu la loi du 21 décembre 1998 'relative à la sécurité lors des matches de football', *Doc. parl.*, Chambre, 1997-1998, n° 1572/1, p. 50 ; avis n° 29.125/4 donné le 14 avril 1999 sur un projet devenu l'arrêté royal du 3 juin 1999 'réglant les modalités de la gestion des billets à l'occasion des matches de football' ; avis n° 37.765/1/2/3/4 donné le 4 novembre 2004 sur un avant-projet devenu la loi-programme du 27 décembre 2004, *Doc. parl.*, Chambre, 2004-2005, n° 1437 ; avis n° 43.186/3 donné le 19 juin 2007 sur un avant-projet devenu le décret du 19 mai 2008 'relatif à l'aide à la Jeunesse et visant la mise en œuvre de mesures de protection de la jeunesse', *Doc. parl.*, Parl. Comm. germ., 2007-2008, n° 120/1 ; avis n° 43.489/4 donné le 10 décembre 2007 sur avant-projet devenu le décret du 30 avril 2009 'relatif à l'information, la coordination et l'organisation des chantiers sous, sur ou au-dessus des voiries ou des cours d'eau', *Doc. parl.*, Parl. wall., 2008-2009, n° 913/1, p. 239 ; avis n° 42.034 donné le 24 janvier 2007 sur un avant-projet de loi 'relatif à certains traitements de données à caractère personnel par le Service Public Fédéral Finances', *Doc. parl.*, Chambre, n° 52-3064/1. Ce dernier avis précise qu'une « simple autorisation d'un comité sectoriel ne saurait

‡LW-BGFSMBJEA-GDCACUQ‡

Par ailleurs, le législateur doit mentionner les personnes ou les institutions autorisées à consulter une base de données [28].

Dans la lignée de ces exigences, l'article 6, paragraphe 3, du RGPD exige, pour les traitements effectués dans le secteur public, que le fondement de ces traitements soient définis « dans le droit de l'État membre auquel le responsable du traitement est soumis ». Et d'ajouter que « les finalités du traitement sont définies dans cette base juridique », celle-ci pouvant contenir « des dispositions spécifiques pour adapter l'application des règles du présent règlement, entre autres : […] les types de données qui font l'objet du traitement ; les personnes concernées ; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être ; la limitation des finalités ; les durées de conservation ; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal […] ».

3. L'article 12 de l'avant-projet est trop flou pour répondre à ces exigences.

Les traitements de données à caractère personnel dont il est question dans cette disposition ne sont pas toujours définis, pas même quant à leurs éléments essentiels. Lorsqu'ils le sont, c'est d'une manière qui manque de clarté.

Comme l'a souligné l'avis de la Commission de la protection de la vie privée, ceci aboutit à accorder un « chèque en blanc » à l'administration.

En particulier, l'on devine que plusieurs traitements de données sont organisés mais ceux-ci ne sont pas clairement mentionnés dans le projet. Par exemple, l'avant-projet mentionne la création d'un « *datawarehouse* », terme anglais non défini si bien que l'on ne perçoit pas quels traitements de données sont concernés. Le commentaire de l'article fait état de « fins de *datamatching* et de *datamining* », mais ces termes, par ailleurs non définis, ne figurent pas dans le texte en projet.

La seule mention selon laquelle les institutions concernées « peuvent [...] recueillir des données à caractère personnel » ne peut suffire à déterminer clairement quelles sont les catégories de données traitées et à vérifier la pertinence et la nécessité de ce recueil au regard des finalités poursuivies.

Le mode de collecte de ces données n'est pas non plus déterminé. On se demande en particulier où ces données vont être puisées. Le texte mentionne l'implication de diverses institutions mais le commentaire de la disposition semble indiquer que ce ne sont pas les seules données de ces institutions qui seront traitées puisque « les données peuvent être puisées dans toute base de données pertinente, publique ou privée, dans le respect des délibérations requises ».

---

suffire » pour organiser « la communication de données à caractère personnel par le SPF Finances à des professions ou des États étrangers ».

[28] Avis n° 43.186/3 donné le 19 juin 2007 sur un avant-projet devenu le décret du 19 mai 2008 'relatif à l'aide à la Jeunesse et visant la mise en œuvre de mesures de protection de la jeunesse', *Doc. parl.*, Parl. Comm. germ., 2007-2008, n° 120/1 ; avis n° 43.489/4 donné le 10 décembre 2007 sur avant-projet devenu le décret du 30 avril 2009 'relatif à l'information, la coordination et l'organisation des chantiers sous, sur ou au-dessus des voiries ou des cours d'eau', *Doc. parl.*, Parl. wall., 2008-2009, n° 913/1.

‡LW-BGFSMBJEA-GDCACUQ‡

L'article 5*bis*, alinéa 2, en projet de la loi du 15 janvier 1990 mentionne certes que les délibérations de la chambre compétente du comité de sécurité de l'information « déterminent la nature des données communiquées ». Néanmoins, comme le souligne également l'avis de la Commission de la protection de la vie privée, si cette procédure n'est pas inutile, elle ne constitue toutefois pas une base légale définissant les données traitées.

Les finalités des différents traitements ne sont pas déterminées.

Aucun responsable de traitement pour ce « *datawarehouse* » n'est désigné.

La réutilisation des données et leur communication à ce « *datawarehouse* » ne sont pas non plus organisées clairement. Quelle va être la fréquence de ces réutilisations de données ? Ces réutilisations entrent-elles dans les missions de l'administration qui communique ces données et du « *datawarehouse* » qui les reçoit (dont on ne connait pas l'objectif) ? S'agit-il de réutiliser des données à des fins distinctes de celles pour lesquelles elles ont été collectées (par exemple, réutiliser à des fins de contrôle des données collectées initialement pour l'octroi d'une allocation ou la gestion d'un dossier administratif) ?

La notion d'« indicateurs de risques » figure également dans le texte à l'examen, sans qu'il indique de quoi il s'agit exactement ni qui les définit.

Il est également question d'« analyses ». On se demande en quoi consistent ces analyses fondées sur des traitements de données, par qui elles sont effectuées et dans quel but.

S'agissant des « données relationnelles en provenance de différentes instances », les questions suivantes se posent : qu'est-ce qu'une « donnée relationnelle », qui sont les « différentes instances » et quelles sont les finalités poursuivies ?

4. La notion d'« indicateurs de risques de fraude », bien que non définie dans le texte, évoque l'idée du recours à la technique du profilage, comme le mentionne également l'avis de la Commission de la protection de la vie privée [29].

L'article 4, 4), du RGPD définit le profilage comme suit :

> « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».

En d'autres termes, le profilage consiste à soumettre les données à caractère personnel du citoyen à un logiciel de calculs, capable d'effectuer notamment des comparaisons et des corrélations statistiques. En fonction du résultat de ces calculs, l'individu est rattaché à une catégorie prédéterminée de la population, qui présente des caractéristiques spécifiques justifiant

[29] § 32.

‡LW-BGFSMBJEA-GDCACUQ‡

qu'on lui réserve une attitude particulière, comme, par exemple, une inspection fiscale pour les fraudeurs fiscaux présumés [30].

L'article 22, paragraphe 1, du RGPD affirme qu'il est en principe interdit de soumettre une personne à « une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire ». Il est fait exception à cette interdiction notamment lorsque, en vertu de l'article 22, paragraphe 2, b), du même règlement, « la décision est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et des libertés et des intérêts légitimes de la personne concernée ». À noter également que les données sensibles visées à l'article 9, paragraphe 1, du RGPD ne peuvent pas faire l'objet d'une telle décision, même dans l'hypothèse visée par l'article 22, paragraphe 2, b), sauf dans l'hypothèse de l'article 9, paragraphe 2, g) (traitement nécessaire pour des motifs d'intérêt public important) et à la condition que « des mesures appropriées pour la sauvegarde des droits et des libertés et des intérêts légitimes de la personne concernée ne soient en place ».

Si, par la création d'un « *datawarehouse* » et le recours à des techniques de « *datamatching* » et « *datamining* », l'intention du législateur est bien de recourir à la technique du profilage, les garanties adéquates doivent être mises en place.

Il y a lieu d'être particulièrement attentif aux droits des personnes concernées par une décision fondée sur la technique du profilage. En effet, l'utilisation du profilage dans le secteur public présente des risques. Le nombre de données traitées en provenance de l'ensemble des administrations est tellement important que des erreurs sont inévitables. Or, ces erreurs peuvent avoir un impact important puisque l'individu dont le profil est affecté d'une erreur sera assimilé à une catégorie de la population qui ne lui correspond pas en réalité. Il sera alors soumis, parfois à de multiples reprises, à des décisions discriminatoires qui le privent injustement de biens ou de services auxquels il aurait pu prétendre sans cette erreur [31]. Récemment, la Cour constitutionnelle a d'ailleurs rappelé que,

> « lorsqu'on recourt à cette technique, il est […] primordial d'utiliser les bons critères de sélection (ensemble de caractéristiques) pour renforcer la lutte contre la fraude sociale (les 'signaux d'alerte' ou 'indicateurs de risque'). Cette technique présente en effet des inconvénients sérieux, *a fortiori* lors de la phase initiale de sa mise en œuvre, ce qui nécessite de faire une évaluation et un suivi permanents des critères (voir Commission de la protection de la vie privée, avis 24/2015, p. 7 ; avis 05/2016, p. 6) » [32].

Et d'ajouter que

[30] M. HILDEBRANDT, « Who is Profiling Who ? Invisible Visibility », *in* S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne et S. Nouwt (éds.), *Reinventing Data Protection ?*, Dordrecht, Springer, 2009, p. 241 ; V. PAPAKONSTANTINOU, « A Data Protection Approach to Data Matching Operations Among Public Bodies », *International Journal of Law and Information Technology*, 2001, vol. 9, n° 1, pp. 62 et 63 ; J.-M. DINANT, C. LAZARO, Y. POULLET, N. LEFEVER et A. ROUVROY, « L'application de la Convention 108 au mécanisme de profilage. Eléments de réflexion destinés au travail futur du Comité consultatif », mars 2008, T-PD (2008) 01, p. 5.

[31] Recommandation CM/Rec(2010)13 du Comité des Ministres aux États membres 'sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage', 23 novembre 2010. Voir également le point 72 de l'exposé de motifs de cette recommandation.

[32] C.C., 15 mars 2018, n° 29/2018, B.3.5.

‡LW-BGFSMBJEA-GDCACUQ‡

> « cette technique de traitement comporte […] des risques […] en ce qu'elle peut notamment amener à établir de fausses corrélations entre les caractéristiques d'un comportement déterminé et des personnes. Le législateur doit donc prévoir des garanties suffisantes » [33],

ce qui suppose notamment la désignation dans la loi du responsable de traitement, la mise en place d'un traitement proportionné, le respect des droits des personnes concernées et notamment le respect du droit d'accès aux données dès que les besoins d'une enquête ne justifient plus que ce droit soit suspendu, ainsi que la mise en place de voies de recours adéquates.

Au vu des risques que des erreurs soient commises dans l'application d'un profil à une personne concernée, le droit à la limitation du traitement, notamment, devrait être mis en œuvre, en ce qu'il permet à une personne qui se verrait attribuer un profil affecté d'une erreur d'en empêcher le traitement le temps de faire corriger cette erreur. Il est consacré à l'article 18 du RGPD. Or, l'article 5*quater* en projet de la loi du 15 janvier 1990 déroge à cet article 18 « lorsque et dans la mesure où des données sociales à caractère personnel sont traitées » [34].

5. En conclusion, la création d'un « *datawarehouse* » traitant un grand nombre de données et concernant une grande partie, voire la totalité des citoyens et recourant éventuellement à des techniques de profilage ne peut être considérée comme anodine. Elle doit donc à tout le moins faire l'objet des mesures d'encadrement dont il est question dans les observations qui précèdent.

Article 13

Les termes de l'article 5*ter* en projet de la loi du 15 janvier 1990 ne répondent pas aux exigences de légalité et de prévisibilité.

Il s'agit en particulier des termes « toute donnée à caractère personnel », « exécution de leurs missions légales » et « dans le cadre de l'exécution d'une autre mission légale ». Il pourrait s'agir d'un traitement ultérieur incompatible avec les finalités poursuivies lors de la collecte, ce que proscrit l'article 5, paragraphe 1, b), du RGPD. Comme l'affirme le considérant n° 50 du RGPD,

> « si le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, le droit de l'Union ou le droit d'un État membre peut déterminer et préciser les missions et les finalités pour lesquelles le traitement ultérieur devrait être considéré comme compatible et licite ».

De telles précisions font défaut en l'espèce.

[33] *Ibid.*, B.31.

[34] Il est également renvoyé à l'observation formulée sur l'article 14.

‡LW-BGFSMBJEA-GDCACUQ‡

Article 14

Les termes de l'article 5*quater* en projet de la loi du 15 janvier 1990 ne répondent pas aux exigences de légalité et de prévisibilité.

La disposition déroge au droit à la limitation du traitement sans énoncer les hypothèses concernées.

Par ailleurs, les catégories de données visées par cette limitation souffrent également d'imprécision, le texte usant du terme « notamment » au moment d'énoncer ces catégories.

Article 19

L'article 15, § 1er, seconde phrase, en projet de la loi du 15 janvier 1990 ne précise pas les critères encadrant l'habilitation donnée au Roi.

Le paragraphe 2, alinéa 6, en projet prévoit une exception à l'obligation d'obtenir l'autorisation du comité, que l'auteur de l'avant-projet doit être en mesure de justifier.

Au paragraphe 3 en projet, la section de législation s'étonne que le comité soit habilité à se prononcer sur l'utilisation du numéro d'identification au registre national alors que celui-ci est une donnée à caractère personnel émanant de la source authentique « Registre national », dont la responsabilité est assumée par le SPF Intérieur.

Article 40

À supposer que l'auteur de l'avant-projet conçoive la chambre « sécurité sociale et santé » comme une autorité administrative indépendante [35], l'article 46 en projet de la loi du 15 janvier 1990 appelle l'observation suivante.

Dans un avis n° 42.387/VR du 27 mars 2007, la section de législation a rappelé ce qui suit :

> « […] concernant l'attribution d'un pouvoir réglementaire à une autorité non politiquement responsable, le Conseil d'État, section de législation, a déjà observé à plusieurs reprises dans le passé que l'attribution d'une compétence réglementaire à des organismes publics ou à leurs organes est difficilement compatible avec les principes généraux du droit public belge, en ce qu'elle porte atteinte au principe de l'unité du pouvoir réglementaire et échappe à tout contrôle parlementaire direct. Les actes réglementaires de ce type sont en outre dépourvus des garanties dont est assortie la réglementation classique, telles que celles en matière de publication et de contrôle préventif exercé par la section de législation du Conseil d'État.
>
> Si dans le passé, le Conseil d'État, section de législation, a déjà jugé admissibles certaines exceptions à l'interdiction de déléguer une compétence réglementaire à des

[35] Il est renvoyé sur ce point à l'observation générale D.

‡LW-BGFSMBJEA-GDCACUQ‡

organismes publics, il s'agissait généralement de délégations de portée limitée et d'une technicité telle que l'on pouvait considérer que les organismes qui devaient appliquer la réglementation concernée, étaient également les mieux placés pour l'élaborer en connaissance de cause et exercer la compétence ainsi déléguée » [36].

L'admissibilité d'une délégation de pouvoir réglementaire à une autorité administrative indépendante est donc [37] subordonnée à des conditions restrictives. L'avis n° 44.607/1 du 12 juin 2008 [38], entre autres [39], énonce à ce sujet que [40] :

« de decreetgever in beginsel enkel aan de regering normatieve bevoegdheden vermag te verlenen, omdat uitgesloten is dat de verordenende macht wordt uitgeoefend op een andere wijze dan is voorgeschreven door de Grondwet.

Deze grondwettelijke regels betekenen niet dat er geen enkele ruimte zou zijn voor een medewerking van andere instanties bij de verordenende bevoegdheid. Evenwel mogen daarbij de grondwettelijke regels betreffende de uitoefening van de normatieve functie niet worden miskend. Het grondwettigheidsbezwaar tegen het laten vaststellen van regels door instanties die geen politieke verantwoordelijkheid dragen, worden opgevangen wanneer aan het uitvoerend orgaan ten aanzien van die regels een goedkeuringsbevoegdheid wordt toegekend die zo is opgevat dat geen afbreuk wordt gedaan aan de genoemde grondwettelijke regels; daarenboven mag het aangewende procédé er niet toe leiden dat de regering wordt belemmerd in de uitoefening van de haar toekomende prerogatieven op normatief vlak […]. Een zulkdanige fragmentering van de verordeningsmacht van het uitvoerend orgaan, die er op neerkomt dat de regering het initiatiefrecht en ook de vrije appreciatie van de maatregelen die nodig zijn voor de uitvoering van het decreet ontnomen wordt, is in strijd met artikel 33 van de Grondwet ».

[36] Avis n° 42.387/VR donné le 27 mars 2007 sur un avant-projet devenu la loi du 15 mai 2007 'portant assentiment à l'accord de coopération entre l'Autorité fédérale, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale relatif à la mise en oeuvre de certaines dispositions du Protocole de Kyoto, conclu à Bruxelles, le 19 février 2007', *Doc. parl.*, Sénat, 2006-2007, n° 3-2411/1, p. 34.

[37] Sans qu'il soit besoin ici d'évoquer la question de l'incidence que pourrait avoir, sur cette admissibilité, l'existence d'obligations issues du droit dérivé de l'Union européenne (voir sur ce point, l'avis n° 50.003/4 donné le 26 septembre 2011 sur un avant-projet devenu la loi du 10 juillet 2012 'portant des dispositions diverses en matière de communications électroniques').

[38] Avis n° 44.607/1 donné le 12 juin 2008 sur un avant-projet devenu le décret du 10 juillet 2008 'betreffende het stelsel van leren en werken in de Vlaamse Gemeenschap', *Doc. parl.*, Parl. fl, 2007-2008, n° 1760/1, pp. 241 à 265.

[39] Voir aussi l'avis n° 50.217/4 donné le 21 septembre 2011 sur un projet devenu l'arrêté royal du 2 décembre 2011 'concernant les infrastructures critiques dans le sous-secteur du transport aérien'.

[40] Voir également J. VANDE LANOTTE, G. GOEDERTIER, Y. HAECK, J. GOOSSENS et T. De PELSMAEKER, *Belgisch Publiekrecht*, vol. 1, Bruges, Die Keure, 2015, pp. 148 et 149.

‡LW-BGFSMBJEA-GDCACUQ‡

L'article 46, § 2, en projet de la loi du 15 janvier 1990 prévoit que les délibérations du comité de sécurité de l'information ont « une portée générale contraignante envers les tiers » et qu'elles ne peuvent être contraires aux normes juridiques supérieures. L'exposé des motifs précise à ce sujet que

> « les délibérations du Comité ont valeur normative (loi matérielle), conformément à l'ordre constitutionnel et peuvent être contestées par les voies de recours en vigueur si elles sont contraires aux normes juridiques supérieures ».

Tant en raison de son ampleur que de l'absence de ratification par une autorité politiquement responsable des normes sur lesquelles débouche sa mise en œuvre, pareille délégation de pouvoir réglementaire méconnaît les conditions d'admissibilité ci-avant rappelées.

L'article 46, § 2, en projet de la loi du 15 janvier 1990 sera fondamentalement revu à la lumière de cette observation.

La même observation vaut pour l'article 35/1, § 1er, en projet de la loi du 15 août 2012 (article 80 de l'avant-projet).

Article 47

S'il pouvait se comprendre que l'article 6 actuellement en vigueur de la loi du 21 août 2008 'relative à l'institution et à l'organisation de la plate-forme eHealth et portant des dispositions diverses' réserve l'applicabilité de la loi du 8 décembre 1992, pareille précaution n'est plus nécessaire pour ce qui concerne l'applicabilité, qui est de droit, du RGPD.

La référence à ce règlement sera omise de l'article 6 en projet, de la loi du 21 août 2008, de manière à ne plus réserver que l'applicabilité de la loi du 22 août 2002 'relative aux droits du patient' et des « dispositions légales et réglementaires relatives à l'exercice de l'art de guérir ».

Articles 60 à 68

1. Les articles 60 à 68 de l'avant-projet entendent mettre en œuvre l'article 23 du RGPD, qui autorise les États membres à limiter la portée des droits et obligations des personnes concernées, prévus par le RGPD.

L'État membre a l'obligation, dans ce cadre, d'adopter des dispositions spécifiques relatives aux différents points listés par l'article 23, paragraphe 2, du RGPD.

L'article 23, paragraphe 2, f), du RGPD impose l'adoption de mesures spécifiques relatives « aux durées de conservation et aux garanties applicables en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement ».

Le dispositif sera complété en ce sens.

‡LW-BGFSMBJEA-GDCACUQ‡

2. Aux articles 100/14, § 3, alinéa 6, 100/15, § 3, alinéa 6, 100/13, § 3, alinéa 6, et 100/17, § 3, alinéa 6, en projet du Code pénal social (articles 62, 64, 66 et 67 de l'avant-projet), il convient de viser plus généralement l'ensemble des possibilités d'action du ministère public.

3. Les mêmes observations valent *mutatis mutandis* pour les articles 71 à 79 de l'avant-projet.

Articles 71 à 79

À l'heure actuelle, la dérogation aux droits des personnes concernées en matière de vie privée pour le Service public fédéral Finances est organisé par l'article 3, § 7, de la loi du 8 décembre 1992.

Cette disposition prévoit uniquement une dérogation concernant l'article 10 (droit d'accès) de la loi du 8 décembre 1992. Aucune dérogation à l'article 9 (droit d'information) ou à l'article 12 (droit de rectification) n'est organisée.

L'auteur de l'avant-projet doit dès lors être en mesure de justifier le fait que de telles possibilités de dérogations sont désormais nécessaires.

Articles 82 et 83

Les articles 82 et 83 de l'avant-projet entendent mettre en œuvre l'article 23 du RGPD, qui autorise les États membres à limiter la portée des droits et obligations des personnes concernées prévus par le RGPD.

Comme le relève l'avis de la Commission de la protection de la vie privée, l'article XV.10/1 du Code de droit économique en projet (article 82 de l'avant-projet) prévoit une limitation extrêmement large des droits de la personne concernée. C'est en effet l'ensemble des droits repris par le chapitre III « Droit de la personne concernée » (articles 12 à 22 du RGPD, ainsi que l'article 34 dudit RGPD, relatif à la « communication à la personne concernée d'une violation de données à caractère personnel »), qui sont exclus nécessairement et systématiquement en cas de traitement de données à caractère personnel par les services d'inspection et/ou de contrôle dont les compétences sont définies par le Code de droit économique.

Si l'article 23 du RGPD permet la limitation de la portée des droits prévus par les articles 12 à 22 et 34 du RGPD, il exige également que l'État membre justifie pour ce faire d'un objectif légitime au sens de l'article 23, paragraphe 1er, du RGPD et qu'« une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique ». Compte tenu de son caractère dérogatoire, cette disposition doit, du reste, faire l'objet d'une interprétation stricte.

‡LW-BGFSMBJEA-GDCACUQ‡

Une ingérence des pouvoirs publics dans l'exercice du droit au respect de la vie privée doit non seulement reposer sur une disposition législative suffisamment précise mais aussi reposer sur une justification raisonnable et être proportionnée aux buts poursuivis par le législateur. Le législateur dispose en la matière d'une marge d'appréciation. Cette marge n'est toutefois pas illimitée : pour qu'une norme soit compatible avec le droit au respect de la vie privée, il faut que le législateur ait établi un juste équilibre entre tous les droits et intérêts en cause.

L'exercice des droits prévus par les articles 12 à 22 et 34 du RGPD participe à l'existence d'un tel équilibre au vu des ingérences dans le droit au respect de la vie privée qui sont autorisées par le RGPD et la loi en projet.

En prévoyant nécessairement et systématiquement, sans même que le service d'inspection ou de contrôle ne doive établir qu'une telle exclusion est nécessaire au bon accomplissement de ses missions (1), l'exclusion totale (2) de l'ensemble (3) des droits prévus par les articles 12 à 22 et 34 du RGPD pour des catégories de traitements – et indirectement des catégories de responsables de traitement – définies de manière très large (4), le législateur ne répond pas à l'exigence de proportionnalité qui s'impose à lui.

L'article 82 de l'avant-projet est rédigé de manière trop large pour avoir permis une mise en balance adéquate des droits en présence afin que les limitations apportées aux droits des personnes concernées ne dépassent pas ce qui est strictement nécessaire à la réalisation de l'objectif légitime poursuivi.

Article 86

L'article 86 s'efforce d'organiser la transition, s'agissant du rôle des comités sectoriels actuels de la Commission de la protection de la vie privée, entre le droit actuellement en vigueur et celui qui résultera de l'adoption de la loi dont l'avant-projet fait l'objet du présent avis.

Il y a toutefois lieu de tenir compte de ce qu'en son principe, la loi-cadre, tel que son avant-projet est en tout cas conçu, dans le prolongement du RGPD, remplace le système d'autorisation par un mécanisme de responsabilisation.

Même si l'avant-projet à l'examen réintroduit le système de l'autorisation par la chambre « sécurité sociale et santé » ou la chambre « autorité fédérale » du comité en ce qui concerne en tout cas les échanges de données concernées par plusieurs dispositions en projet, la volonté du législateur, tel qu'elle résultera des textes qu'il adoptera, à tout le moins s'ils ne sont pas modifiés par rapport à l'avant-projet de loi-cadre et à l'avant-projet, n'apparaîtra pas de manière suffisamment claire quant à la conception qui sera la sienne sur le rôle des organismes appelés à se substituer aux comités sectoriels ; il est renvoyé sur ce point à l'observation générale B.

C'est au législateur lui-même qu'il appartient d'assurer la transition entre le droit actuel et celui en construction, s'agissant notamment du rôle actuel des comités sectoriels.

‡LW-BGFSMBJEA-GDCACUQ‡

Il ne peut laisser ces questions à une démarche interprétative des destinataires des législations en voie d'être adoptées, les fondements des interprétations possibles étant trop incertains.

Article 87

L'article 87 de l'avant-projet tend à conférer au Roi une habilitation Lui permettant de

> « modifier, compléter, remplacer ou abroger les dispositions légales existantes pour les mettre en conformité avec celles contenues dans la présente loi ».

Le commentaire de cette disposition se borne à préciser que celle-ci

> « donne la compétence au Roi d'adapter les dispositions légales éventuelles qui ne sont pas en conformité avec cette loi. Ces adaptations ne peuvent pas avoir trait à la loi cadre *privacy* ».

Il va de soi, eu égard notamment au principe de la légalité qui découle de l'article 22 de la Constitution, que l'habilitation ainsi prévue, si larges en soient les termes, ne peut que viser la mise en œuvre formelle et légistique des choix qui sont ceux de l'avant-projet de loi à l'examen, et ne peut aboutir à conférer au Roi le pouvoir d'opérer Lui-même de nouveaux choix de fond dans le règlement de la matière.

*

‡LW-BGFSMBJEA-GDCACUQ‡

Aangezien de adviesaanvraag ingediend is op basis van artikel 84, § 1, eerste lid, 2°, van de wetten 'op de Raad van State', gecoördineerd op 12 januari 1973, beperkt de afdeling Wetgeving overeenkomstig artikel 84, § 3, van de voornoemde gecoördineerde wetten haar onderzoek tot de rechtsgrond van het voorontwerp,‡ de bevoegdheid van de steller van de handeling en de te vervullen voorafgaande vormvereisten.

Wat die drie punten betreft, geeft het voorontwerp aanleiding tot de volgende opmerkingen.

ALGEMENE OPMERKINGEN

A. Het recht op eerbiediging van het privéleven

1. Zoals het Grondwettelijk Hof recent nog opgemerkt heeft[1] in verband met het recht op eerbiediging van het privéleven dat gewaarborgd wordt door artikel 22 van de Grondwet, gelezen in samenhang met artikel 8 van het Europees Verdrag voor de rechten van de mens, artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten en de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie, is de draagwijdte van artikel 8 EVRM analoog aan die van de voormelde grondwettelijke bepaling, zodat de waarborgen die deze beide bepalingen bieden een onlosmakelijk geheel vormen.

De artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie hebben, wat de verwerking van persoonsgegevens in het kader van de uitvoering van het Unierecht betreft, een draagwijdte die analoog is aan die van artikel 8 van het Europees Verdrag voor de rechten van de mens en aan die van artikel 22 van de Grondwet. Hetzelfde geldt voor artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten.

Het recht op eerbiediging van het privéleven, zoals gewaarborgd in de voormelde grondwets- en verdragsbepalingen, heeft voornamelijk tot doel de personen te beschermen tegen inmengingen in hun privéleven. Dat recht heeft een ruime draagwijdte en omvat onder meer de bescherming van persoonsgegevens en van persoonlijke informatie.

In dat verband en wat de toepassingsgebieden buiten de Europese Unie betreft, wordt in Verdrag nr. 108 van de Raad van Europa van 28 januari 1981 'tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens', dat bindend is voor de Belgische Staat, eveneens bepaald dat de Belgische Staat een reeks minimale waarborgen moet bieden.

2.1. Dat recht is evenwel niet absoluut. Het sluit overheidsinmenging in het recht op eerbiediging van het privéleven niet uit, maar het is vereist dat zij toegestaan wordt door een voldoende precieze wettelijke bepaling, dat zij beantwoordt aan een dwingende maatschappelijke behoefte in een democratische samenleving en dat zij evenredig is met de daarmee nagestreefde

‡ Aangezien het om een voorontwerp van wet gaat, wordt onder "rechtsgrond" de overeenstemming met de hogere normen verstaan.

[1] GwH 14 juli 2016, nr. 108/2016, B.7 tot B.13; 15 maart 2018, nr. 29/2018, B.9 tot B.15.

‡LW-BGFSMBJEA-GDCACUQ‡

wettige doelstelling. Die bepalingen houden voor de overheid bovendien de positieve verplichting in om maatregelen te nemen die een daadwerkelijke eerbiediging van het privéleven verzekeren, zelfs in de sfeer van de onderlinge verhoudingen tussen individuen.

2.2. Doordat artikel 22 van de Grondwet aan de bevoegde wetgever de bevoegdheid voorbehoudt om vast te stellen in welke gevallen en onder welke voorwaarden afbreuk kan worden gedaan aan het recht op eerbiediging van het privéleven, waarborgt het aan elke burger dat geen enkele inmenging in dat recht kan plaatsvinden dan krachtens regels die zijn aangenomen door een democratisch verkozen beraadslagende vergadering. Een delegatie aan een andere macht is evenwel niet in strijd met het wettelijkheidsbeginsel voor zover de machtiging voldoende nauwkeurig is omschreven en betrekking heeft op de tenuitvoerlegging van maatregelen waarvan de essentiële elementen voorafgaandelijk door de wetgever vastgesteld zijn.

In dit verband hebben het Grondwettelijk Hof en de afdeling Wetgeving van de Raad van State reeds verscheidene keren benadrukt dat het democratisch debat een waarborg vormt voor de bescherming van het privéleven van de burgers. Zo stellen zij dat

> "[de Grondwetgever, door] de bescherming van de persoonlijke levenssfeer te laten waarborgen door de wet zelf, (…) de bedoeling gehad [heeft] democratisch verkozen beraadslagende vergaderingen te laten beslissen over de gevallen waarin en de voorwaarden waaronder [daarop] inbreuk (…) kan worden gemaakt".[2]

Er dient voor gezorgd te worden dat de parlementsleden daarbij betrokken worden, aangezien

> "[de wetgever juist] waar de risico's voor de bescherming van de persoonlijke levenssfeer het grootst zijn, (…) op de meest rechtstreekse wijze bij de regelgeving betrokken [zou] moeten worden".[3]

Als de wetgevende macht die taak niet op zich zou nemen, zou dat erop neerkomen dat

> "[de] wetgever, die in de Grondwet is aangewezen als bewaker van het recht op eerbiediging van het [privéleven], ervan [zou] afzien zelf te bepalen welke inmengingen het recht dat hij moet bewaken kunnen komen beknotten. Artikel 22 van de Grondwet verbiedt de wetgever die keuze te maken."[4]

---

[2] Advies 37.765/1/2/3/4, op 4 november 2004 gegeven over een voorontwerp dat geleid heeft tot de programmawet van 27 december 2004, *Parl.St.* Kamer 2004-05, nr. 1437/2 ; adviezen 37.748/AV en 37.749/AV, op 23 november 2004 gegeven over een voorontwerp dat geleid heeft tot de wet van 3 mei 2005 'houdende wijziging van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen' (37.748/AV) en over een voorontwerp dat geleid heeft tot de wet van 3 mei 2005 'houdende wijziging van de wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen' (37.749/AV), *Parl.St.* Kamer 2004-05, nrs. 1598/1 en 1599/1; GwH 21 december 2004, nr. 202/2004, B.4.3 en B.6.3; 26 juni 2008, nr. 95/2008, B.42; 18 maart 2010, nr. 29/2010, B.16.1; 14 februari 2013, nr. 6/2013, B.5.7; 16 mei 2013, nr. 66/2013, B.11.1.

[3] Advies 33.487/1/3 van 18 en 20 juni 2002 betreffende een voorontwerp dat geleid heeft tot de wet van 22 augustus 2002 'houdende maatregelen inzake gezondheidszorg', *Parl.St.* Kamer 2002-03, nr. 2125/2, 539.

[4] Advies 26.198/2, op 2 februari 1998 gegeven over een voorontwerp dat geleid heeft tot de wet van 11 december 1998 'tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens', *Parl.St.* Kamer 1997-98, nr. 49-1566/1, 108.

‡LW-BGFSMBJEA-GDCACUQ‡

2.3. Naast het formele wettelijkheidsvereiste legt artikel 22 van de Grondwet eveneens de verplichting op dat de inmenging in het recht op eerbiediging van het privéleven in duidelijke en voldoende nauwkeurige bewoordingen wordt geformuleerd die het mogelijk maken de hypothesen te voorzien waarin de wetgever een dergelijke inmenging in het recht op eerbiediging van het privéleven toestaat.

Evenzo houdt het vereiste van voorzienbaarheid waaraan de wet moet voldoen om in overeenstemming te worden bevonden met artikel 8 van het Europees Verdrag voor de rechten van de mens, in dat de formulering ervan voldoende precies is zodat eenieder – desnoods met gepast advies – in de gegeven omstandigheden in redelijke mate de gevolgen van een bepaalde handeling kan voorzien. De wetgeving moet eenieder een voldoende indicatie geven over de omstandigheden waarin en de voorwaarden waaronder de overheden gebruik mogen maken van maatregelen die raken aan de rechten gewaarborgd door het Verdrag. Meer in het bijzonder wanneer het optreden van de overheid een geheim karakter vertoont, dient de wet voldoende waarborgen te bieden tegen willekeurige inmengingen in het recht op eerbiediging van het privéleven, namelijk door de beoordelingsbevoegdheid van de betrokken overheden op voldoende duidelijke wijze af te bakenen, enerzijds, en door te voorzien in procedures die een effectief toezicht toelaten, anderzijds.

Uit artikel 8 van het Europees Verdrag voor de rechten van de mens en artikel 22 van de Grondwet volgt aldus dat voldoende precies moet worden bepaald in welke omstandigheden een verwerking van persoonsgegevens is toegelaten. De vereiste graad van precisie van de betrokken wetgeving − die niet in elke hypothese kan voorzien − is, volgens het Europees Hof voor de Rechten van de Mens, onder meer afhankelijk van het domein dat wordt gereguleerd en van het aantal en de hoedanigheid van de personen tot wie de wet gericht is. Zo heeft het Europees Hof voor de Rechten van de Mens geoordeeld dat het vereiste van voorzienbaarheid in domeinen die te maken hebben met de nationale veiligheid, niet dezelfde draagwijdte kan hebben als in andere domeinen.[5]

2.4. Overheidsinmenging in het recht op eerbiediging van het privéleven dient niet alleen te steunen op een voldoende precieze wettelijke bepaling, ze dient daarenboven op een redelijke verantwoording te berusten en evenredig te zijn met de doelstellingen die nagestreefd worden door de wetgever, die ter zake over een appreciatiemarge beschikt. Die appreciatiemarge is evenwel niet onbegrensd: opdat een wettelijke regeling verenigbaar is met het recht op eerbiediging van het privéleven, is vereist dat de wetgever een billijk evenwicht heeft gevonden tussen alle rechten en belangen die in het geding zijn.

Wat de evenredigheid betreft, houden het Europees Hof voor de Rechten van de Mens en het Hof van Justitie van de Europese Unie rekening met het al dan niet aanwezig zijn van materiële en procedurele waarborgen in de betrokken regeling. Bij de beoordeling van de evenredigheid van maatregelen met betrekking tot de verwerking van persoonsgegevens, dient aldus rekening te worden gehouden met, onder meer, het geautomatiseerde karakter ervan, de gebruikte technieken, de accuraatheid, de pertinentie en het al dan niet buitensporige karakter van de gegevens die worden verwerkt, het al dan niet voorhanden zijn van maatregelen die de duur van de bewaring van de gegevens beperken, het al dan niet voorhanden zijn van een systeem van

[5] EHRM 26 maart 1987, *Leander* t. Zweden, § 51; 4 juli 2006, *Lupsa* t. Roemenië, § 33.

‡LW-BGFSMBJEA-GDCACUQ‡

onafhankelijk toezicht dat toelaat na te gaan of de bewaring van de gegevens nog langer is vereist, het al dan niet voorhanden zijn van afdoende controlerechten en rechtsmiddelen voor de betrokkenen, het al dan niet voorhanden zijn van waarborgen ter voorkoming van stigmatisering van de personen van wie de gegevens worden verwerkt, het onderscheidend karakter van de regeling en het al dan niet voorhanden zijn van waarborgen ter voorkoming van foutief gebruik en misbruik van de verwerkte persoonsgegevens door de overheidsdiensten.

3. *In casu* houdt het recht op eerbiediging van het privéleven verband met de kern zelf van het voorontwerp dat aan de afdeling Wetgeving voorgelegd is. Het voorontwerp is dan ook onderzocht in het licht van de beginselen waaraan zonet herinnerd is.

B. De algemene opzet van de wetgeving betreffende de verwerking van persoonsgegevens bij de overheid

1. Dat zowel de federale overheid als de deelstaten het nodig achten specifieke wetgevingen aan te nemen als kader voor bepaalde vormen van gegevensverwerking, valt te begrijpen. Zo vormen, op federaal niveau, een aantal sectorale wetgevingen, zoals de wet van 8 augustus 1983 'tot regeling van een Rijksregister van de natuurlijke personen, de wet van 15 januari 1990 'houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid' en de wet van 19 mei 2010 'houdende oprichting van de Kruispuntbank van de voertuigen' sedert verscheidene jaren het kader voor specifieke vormen van gegevensverwerking in bijzondere overheidssectoren.

Hoewel elk van die overheidssectoren zijn eigen bijzondere kenmerken bezit, delen ze ok gemeenschappelijke bezorgdheden, te beginnen met de zorg voor efficiënt bestuur met eerbiediging van de bescherming van het privéleven van de burgers, en vertonen ze punten van overeenstemming, zoals de middelen die aangewend worden om te komen tot de vormen van gegevensverwerking in kwestie (authentieke gegevensbronnen, dienstenintegrators, identificatiemiddelen, enz.). In dat verband wordt in het voorontwerp van wet waarover de Raad van State op 19 april 2018 advies 63.192/2 uitgebracht heeft, welk voorontwerp strekt tot het aannemen van de kaderwet betreffende de uitvoering van verordening 2016/679/EU 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' (hierna: "de kaderwet"), een afzonderlijke afdeling aan de publieke sector gewijd, met gemeenschappelijke begrippen en regels.[6]

De kwestie van de uitwisseling van gegevens tussen overheidsdiensten is een van de zaken die de onderscheiden overheidssectoren gemeen hebben. Die kwestie wordt overigens aangesneden in het voorontwerp van kaderwet waarvan *supra* sprake is en waarin de gegevensuitwisseling geregeld wordt door middel van een gemeenschappelijke regel voor de publieke sector en protocollen betreffende de uitwisseling van gegevens tussen verantwoordelijken voor de verwerking van persoonsgegevens.

[6] Wanneer verderop in dit advies sprake is van de kaderwet, gaat het om opmerkingen die geformuleerd zijn op grond van de inhoud van die kaderwet zoals ze als voorontwerp aan de afdeling Wetgeving voorgelegd is.

‡LW-BGFSMBJEA-GDCACUQ‡

Met het voorliggend voorontwerp wordt evenwel afgeweken van die gemeenschappelijke regel en wordt een instantie opgericht die lijkt op die welke thans gevormd worden door de sectorale comités die afgeschaft worden bij de wet van 3 december 2017 'tot oprichting van de Gegevensbeschermingsautoriteit', welke wet grotendeels op 25 mei 2018 in werking treedt. Noch de tekst van het voorontwerp, noch de memorie van toelichting van de kaderwet leveren grond op om een vorm van toezicht in te voeren naast die waarin de kaderwet zelf voorziet of om ervan uit te gaan dat het nodig zou zijn opnieuw een sectoraal comité in het leven te roepen.

In het licht van deze vaststellingen zou de samenhang tussen het voorontwerp van kaderwet en het voorliggend voorontwerp opnieuw nagegaan moeten worden.

2. Overigens vertoont de vorm van toezicht die bij het voorontwerp ingevoerd wordt een gebrek aan samenhang ten opzichte van die welke bij het voorontwerp van kaderwet geregeld wordt voor de verwerking van gegevens die in de publieke sector verricht wordt.

In het bijzonder wekt het verbazing dat eenzelfde wetgever, ter gelegenheid van het regelen van de vormen van uitwisseling van gegevens tussen overheidsdiensten, tegelijkertijd aan de verantwoordelijken voor de verwerking in de publieke sector extra verantwoordelijkheden wil opdragen bij de ene wet en aan hen iedere verantwoordelijkheid wil ontnemen bij een andere wet. In de thans ontworpen kaderwet, meer in het bijzonder in de afdeling die specifiek aan de publieke sector gewijd is (artikel 22), worden aan de verantwoordelijken voor de gegevensverwerking immers extra verantwoordelijkheden toegekend doordat hen de mogelijkheid geboden wordt om, met de hulp van hun functionaris voor gegevensbescherming, onderling protocollen voor gegevensuitwisseling af te sluiten, terwijl bij het voorliggend voorontwerp aan de verantwoordelijken voor de gegevensverwerking alle verantwoordelijkheid ontnomen wordt, aangezien daarbij een orgaan opgericht wordt dat vooraf toezicht uitoefent en dat, in de gevallen bedoeld in het ontworpen artikel 15, § 1, van de wet van 15 januari 1990 (artikel 19 van het voorontwerp) en in het ontworpen artikel 35/1, § 1, derde lid, van de wet van 15 augustus 2012 'houdende oprichting en organisatie van een federale dienstenintegrator' (artikel 80 van het voorontwerp), vooraf en in de plaats van de verwerkingsverantwoordelijken de gegevensuitwisseling toestaat of weigert. Dat aan de verwerkingsverantwoordelijken alle verantwoordelijkheid ontnomen wordt, blijkt ook op het stuk van de indienstneming en het functioneren van de functionaris voor gegevensbescherming, die geacht wordt door de verwerkingsverantwoordelijke in dienst te worden genomen en zijn functies vervolgens op onafhankelijke wijze uit te oefenen, aangezien het in het voorliggend voorontwerp, volgens de bespreking van artikel 40, zo is dat "[het] informatieveiligheidscomité (…) ook tussen[komt] bij de aanwijzing en bij de opvolging van functionarissen voor gegevensbescherming (…) om (…) op [te] volgen of [de betrokkene] zijn functie naar behoren kan uitoefenen (bijvoorbeeld inzake beschikbare tijd) en de nodige ondersteuning krijgt aangeboden (bijvoorbeeld inzake vorming)".[7]

[7] Zie het ontworpen artikel 46, § 1, 8°, van de wet van 15 januari 1990 (artikel 40 van het voorontwerp).

‡LW-BGFSMBJEA-GDCACUQ‡

Die problemen zijn des te acuter, daar deze aangelegenheid, voor een dermate ruim toepassingsgebied, dat immers alle federale overheidsdiensten omvat, anders geregeld zal zijn door twee afzonderlijke gehelen van wetgevingen, te weten enerzijds de kaderwet, en anderzijds de wetten die bij het voorliggend voorontwerp gewijzigd worden.

Uit die twee totaal verschillende benaderingen die vervat zijn in twee voorontwerpen die de regering tegelijk bij het Parlement wil indienen, blijkt niet alleen een gebrek aan alomvattende visie, ze doen eveneens ernstige twijfels rijzen over de vraag of bij de waarborging van het recht op bescherming van het privéleven het gelijkheidsbeginsel wel in acht genomen wordt.

C. De onvolledigheid van het voorontwerp

Bij het voorontwerp wordt het sectoraal comité van de sociale zekerheid en van de gezondheid, dat opgeheven wordt bij de wet tot oprichting van de Gegevensbeschermingsautoriteit, opnieuw tot leven gewekt met de oprichting van het informatieveiligheidscomité.

De bedoeling van de steller van het voorontwerp bestaat erin dat comité ertoe te machtigen bestuurlijke beslissingen te nemen (een gegevensuitwisseling toe te staan of te weigeren).[8] Hoofdstuk 2, waarbij dat comité opgericht wordt, bevat weliswaar regels betreffende de samenstelling van dat comité, maar het voorontwerp dient aangevuld te worden met bepalingen waarbij de bevoegdheid van de kamer "federale overheid" op een duidelijke en samenhangende wijze afgebakend wordt, in het bijzonder wat de criteria betreft die, indien daaraan voldaan is, een beslissing van dat comité noodzakelijk maken.[9]

Voorts is niet duidelijk welke doelstellingen door dat toezichtsorgaan nagestreefd worden. De gegevens inzake sociale zekerheid en de gegevens inzake gezondheid circuleren binnen twee afzonderlijke sectorale netwerken, waarin telkens een afzonderlijke dienstenintegrator het centrale punt vormt (de Kruispuntbank van de sociale zekerheid voor het netwerk van de sociale zekerheid en het eHealth-platform voor het netwerk van de gezondheid). Dat is een uitstekende oplossing in het licht van het vereiste van *Privacy by design* dat verankerd is in 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' (hierna te noemen: de AVG"). Daardoor is de administratie immers aldus geconstrueerd dat er een scheiding bestaat tussen onderscheiden gegevens die voor verschillende doeleinden gebruikt worden en wordt het risico afgewend dat onderscheiden gegevens op één enkele plaats samengebracht worden, welke oplossing meer gevaar zou opleveren voor de bescherming van het privéleven. Indien het toezicht op de gegevens inzake sociale zekerheid en de gegevens inzake gezondheid aan hetzelfde orgaan en aan dezelfde kamer binnen dat orgaan

[8] Wat dit punt betreft, wordt eveneens verwezen naar de opmerking die bij artikel 40 gemaakt wordt.

[9] Voor de kamer "sociale zekerheid en gezondheid" worden de bevoegdheden bepaald bij het ontworpen artikel 46 van de wet van 15 januari 1990 (artikel 40 van het voorontwerp).

‡LW-BGFSMBJEA-GDCACUQ‡

zou worden toegewezen, lijkt dat het vereiste van *Privacy by design* aan te tasten. In het voorontwerp wordt voor die keuze evenwel geen verantwoording gegeven.

Is het, nog steeds wat de doelstellingen van dat toezicht betreft, de bedoeling om uitsluitend toezicht uit te oefenen op het gebruik van de bedoelde gegevens of ook op de werkwijze van de socialezekerheids- en gezondheidsinstellingen? Het wekt verbazing vast te stellen dat bij het ontworpen artikel 46, § 1, 7° en 8°, van de wet van 15 januari 1990 (artikel 40 van het voorontwerp) aan het comité de taak toevertrouwd wordt om zich te mengen in de aanwijzing van de functionaris voor gegevensbescherming van de Kruispuntbank en op zijn werk toe te zien, en na te gaan of de functionarissen voor gegevensbescherming hun functie naar behoren kunnen uitoefenen, met de nodige ondersteuning.

Ten slotte wordt in de bespreking van het ontworpen artikel 46 van de wet van 15 januari 1990 (artikel 40 van het voorontwerp) uiteengezet dat de beslissingen van het comité bindend zijn ten aanzien van derden, dat daartegen bij de Raad van State beroep ingesteld kan worden en dat ze gepubliceerd worden. In het dispositief staat evenwel niets over de bekendmaking van de beslissingen van het comité.

Die grote leemten en die welke in de bijzondere opmerkingen ter sprake zullen komen, dienen opgevuld te worden.

D. Het statuut van het informatieveiligheidscomité

1. Er komt niet duidelijk tot uiting welk statuut het informatieveiligheidscomité zal bezitten, wat vragen doet rijzen, zowel in het licht van de Grondwet als in het licht van de AVG.

2. Uit de memorie van toelichting en uit verscheidene bepalingen van het voorontwerp blijkt dat het de bedoeling is dat dit comité en de beide kamers waaruit het bestaat de opvolger worden en "de bevoegdheden overnemen" van het sectoraal comité van de sociale zekerheid en van de gezondheid, enerzijds, en van het sectoraal comité voor de federale overheid, anderzijds, die beide binnen de Commissie voor de bescherming van de persoonlijke levenssfeer opgericht zijn.[10]

Anders dan die beide sectorale comités zal het informatieveiligheidscomité niet opgericht worden binnen de Gegevensbeschermingsautoriteit, dat krachtens de wet van 3 december 2017 'tot oprichting van de Gegevensbeschermingsautoriteit' de opvolger van de Commissie voor de bescherming van de persoonlijke levenssfeer wordt. In de memorie van toelichting wordt bovendien gesteld dat de bedoeling van de steller van het voorontwerp er niet in bestaat om van dat comité een "toezichthoudende autoriteit" in de zin van de AVG, te maken, te weten een "door een lidstaat (…) ingestelde onafhankelijke overheidsinstantie" die "verantwoordelijk [is] voor het toezicht op de toepassing van deze verordening, teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met de verwerking

[10] Artikel 37 van de wet van 15 januari 1990 en artikel 36*bis* van de wet van 8 december 1992 'tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens'.

‡LW-BGFSMBJEA-GDCACUQ‡

van hun persoonsgegevens te beschermen en het vrije verkeer van persoonsgegevens binnen de Unie te vergemakkelijken"[11]

In verscheidene bepalingen van het voorontwerp wordt de bedoeling van de steller ervan tot uiting gebracht om van dit comité een onafhankelijke administratieve overheid te maken die, onder andere, toestemming kan verlenen voor onderscheiden vormen van verwerking van persoonsgegevens die door de overheidsdiensten verricht worden en zelfs, in bepaalde gevallen, regels kan vaststellen die bij deze vormen van verwerking gevolgd moeten worden.[12]

Indien het de bedoeling is dat dit comité dergelijke beslissingen neemt en indien het niet zelf een toezichthoudende autoriteit in de zin van de AVG is, dient dat comité in het licht van die verordening blijkbaar beschouwd te worden als een "verwerkingsverantwoordelijke".

Een "verwerkingsverantwoordelijke" wordt in artikel 4, punt 7, van de AVG immers gedefinieerd als

> "een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen".

Aangezien bepaalde "beraadslagingen" (bedoeld wordt blijkbaar: "besluiten") die door het comité genomen moeten worden, ertoe strekken te bepalen voor welke doeleinden en met welke middelen overheidsdiensten gegevens mogen verwerken, dient dit comité, als het zelf geen toezichthoudende autoriteit is, dan ook onder het toezicht van een "toezichthoudende autoriteit" te worden geplaatst. Hoewel de AVG wel bepaalde afwijkingen wegens taken van algemeen belang[13] toestaat, staat ze immers niet toe dat de verwerkingsverantwoordelijken[14] buiten de bevoegdheid van een toezichthoudende autoriteit zouden vallen.

3. Uit verscheidene bepalingen van het voorontwerp blijkt dat dit comité gemachtigd zal zijn beslissingen te nemen die "een algemene bindende draagwijdte jegens derden" hebben.[15] Gelet op de onduidelijkheid die heerst omtrent de normen die dat comité ten uitvoer zal moeten leggen, zal dat comité over een ruime discretionaire bevoegdheid beschikken. Bij de uitoefening van die bevoegdheid zal dat comité evenwel onder geen enkele hiërarchische controle of enig toezicht vanwege de uitvoerende macht ressorteren. Er wordt zelfs uitdrukkelijk bepaald dat de leden van dat comité van niemand onderrichtingen mogen krijgen.[16]

[11] Artikelen 4, punt 21, en 51, lid 1, van de AVG.

[12] Zie, inzonderheid, artikel 40 en, in dit advies, de bijzondere opmerking die bij die bepaling gemaakt wordt.

[13] Artikel 23 van de AVG.

[14] Met uitzondering van de verwerkingen door gerechten bij de uitoefening van hun rechterlijke taken (artikel 55 van de AVG).

[15] Ontworpen artikel 46, § 2, van de wet van 15 januari 1990 (artikel 40 van het voorontwerp).

[16] Artikel 5 van het voorontwerp.

‡LW-BGFSMBJEA-GDCACUQ‡

Die beslissingen zullen dus bindend zijn voor eenieder, en inzonderheid voor degenen wier persoonsgegevens verwerkt mogen worden krachtens een toestemming vanwege dat comité. Die personen beschikken weliswaar nog steeds over de mogelijkheid om beslissingen die volgens hen in strijd zijn met hogere normen, aan te vechten door middel van een jurisdictioneel beroep, maar hun wordt de garantie ontnomen dat beslissingen met betrekking tot hen genomen worden door een politiek verantwoordelijke overheidsinstantie.

Zowel de afdeling Wetgeving als het Grondwettelijk Hof hebben weliswaar reeds aanvaard dat onafhankelijke administratieve overheidsinstanties opgericht werden, inzonderheid wanneer een Europese regeling dat voorschrijft.[17] *In casu* wordt bij de AVG evenwel een verplichting inzake onafhankelijkheid opgelegd aan de toezichthoudende autoriteit en niet aan de overheidsinstanties die persoonsgegevens verwerken of dergelijke verwerkingen toestaan zonder dat ze het statuut van een dergelijke toezichthoudende autoriteit krijgen, en die net onder het toezicht van de toezichthoudende autoriteit moeten worden geplaatst. Doordat het comité gemachtigd wordt tot het nemen van beslissingen inzake de verwerking van persoonsgegevens die voor derden bindend zijn, terwijl de vraag of dergelijke beslissingen, zelfs gesteld dat ze conform de hogere normen zijn, wel opportuun zijn niet ter toetsing aan een politiek verantwoordelijke overheidsinstantie voorgelegd kan worden, ontzegt het voorontwerp de personen in kwestie de garantie van een dergelijke toetsing, zonder dat zulks te rechtvaardigen valt op grond van een vereiste van een hogere norm, zoals een Europese norm.

Bijgevolg is het van tweeën één:

– ofwel wordt het informatieveiligheidscomité opgericht als een toezichthoudende autoriteit in de zin van de AVG (of wordt het opgericht binnen de Gegevensbeschermingsautoriteit), waarbij, in voorkomend geval zijn taken aangepast worden en zijn onafhankelijkheid versterkt wordt;[18]

– ofwel behoudt dat comité de bevoegdheden die hieraan bij de wet zijn toegekend als orgaan dat betrokken wordt bij de beslissingen van de overheidsdiensten inzake de verwerking van persoonsgegevens, in welk geval er geen enkele reden is om dat comité niet zowel onder de hiërarchische controle of het toezicht van de uitvoerende macht te plaatsen [19] als onder het toezicht van de Gegevensbeschermingsautoriteit of van een andere toezichthoudende autoriteit die opgericht zou zijn met naleving van hoofdstuk VI van de AVG.

*

[17] Zie inz. advies 50.003/4, gegeven op 26 september 2011, over een voorontwerp dat geleid heeft tot de wet van 10 juli 2012 'houdende diverse bepalingen inzake elektronische communicatie', *Parl.St.* Kamer 2011-12, nr. 53-2143/1, 169 tot 234, en de rechtspraak van het Grondwettelijk Hof waarnaar in dat advies verwezen wordt.

[18] Zo wordt bij artikel 3 niet verboden dat de leden van de kamer sociale zekerheid en gezondheid onder het hiërarchisch gezag staan van een andere minister dan de minister bevoegd voor de sociale zekerheid of de volksgezondheid. Bij het ontworpen artikel 42 van de wet van 15 januari 1990 (artikel 35 van het voorontwerp) worden de overheidsdiensten in kwestie betrokken bij de voorbereiding van de besluiten die het comité dient te nemen, wat niet in overeenstemming zou zijn met artikel 52, lid 5, van de AVG, betreffende de onafhankelijkheid van de toezichthoudende autoriteit.

[19] Het voorontwerp bevat geen enkele bepaling in die zin.

‡LW-BGFSMBJEA-GDCACUQ‡

Deze algemene opmerkingen strekken ertoe de wetgever te verzoeken om nu reeds op een zo homogeen en zo geharmoniseerd mogelijke wijze de algemene structuur te bepalen van de wetgeving die, uitgaande van de kaderwet en door middel van opeenvolgende bijzondere wetten, samen met de AVG het recht zal vormen dat van toepassing is op de verwerking van gegevens door de federale publieke sector, van welke structuur het voorliggend voorontwerp het eerste element zou zijn dat volgt na het aannemen van de kaderwet (algemene opmerking B).

In deze algemene opmerkingen wordt tevens vastgesteld dat het voorontwerp ernstige gebreken vertoont (algemene opmerking C).

Ten slotte wordt daarin de vraag gesteld wat het statuut van het informatieveiligheidscomité is en hoe dat statuut zich verhoudt tot de bevoegdheden van de Gegevensbeschermingsautoriteit (algemene opmerking D).

Onder voorbehoud van die algemene opmerkingen wordt dit advies gegeven.

BIJZONDERE OPMERKINGEN

DISPOSITIEF

Hoofdstuk 2 – Oprichting van het Informatieveiligheidscomité

Aangezien de bevoegdheden van het "Informatieveiligheidscomité" zich niet beperken tot de veiligheid van de informatie maar de uitoefening van het toezicht op de naleving van het geheel van de regels inzake gegevensbescherming behelzen, zou de benaming ervan herzien moeten worden.

Artikel 10

Bij artikel 10 wordt de samensmelting van twee functies geregeld: enerzijds die van veiligheidsconsulent en anderzijds die van functionaris voor gegevensbescherming.

Het gaat echter om twee onderscheiden functies waarmee twee onderscheiden functieprofielen overeenstemmen, in tegenstelling tot wat gesteld wordt in de memorie van toelichting waarin staat dat veiligheidsconsulent het "oud concept" en functionaris voor gegevensbescherming het "nieuw concept" is.

Veiligheidsconsulent is een functie die voor de socialezekerheidsinstellingen in het leven geroepen is bij de wet van 15 januari 1990. Ze wordt beschreven in artikel 25 van die wet, dat luidt als volgt:

> "De veiligheidsconsulent bedoeld in artikel 24, eerste en tweede lid, staat, met het oog op de veiligheid van de sociale gegevens die door zijn instelling worden verwerkt of uitgewisseld en met het oog op de bescherming van de persoonlijke levenssfeer van de personen op wie deze sociale gegevens betrekking hebben, in voor:
>
> 1° het verstrekken van deskundige adviezen aan de persoon belast met het dagelijks bestuur;

‡LW-BGFSMBJEA-GDCACUQ‡

2° het uitvoeren van opdrachten die hem door de persoon belast met het dagelijks bestuur worden toevertrouwd.

De veiligheidsconsulent van de Kruispuntbank verstrekt bovendien deskundige adviezen over de veiligheid van het netwerk.

De Koning kan de regels bepalen volgens welke de veiligheidsconsulenten hun opdrachten uitvoeren.".

De veiligheidsconsulent oefent dus in hoofdzaak een functie uit die gewijd is aan de informaticaveiligheid.

Functionaris voor gegevensbescherming is een functie ingesteld bij artikel 37 en volgende van de AVG. Die functie is gewijd aan de gegevensbescherming in het algemeen, wat een ruimere opdracht is dan de loutere informaticaveiligheid. In lid 5 van artikel 37 van de AVG wordt bovendien vermeld dat de functionaris voor gegevensbescherming inzonderheid aangewezen wordt op grond van "zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming".

De samensmelting van die twee functies roept vragen op ten aanzien van de AVG, inzonderheid ten aanzien van artikel 39 waarin de talrijke taken van de functionaris voor gegevensbescherming worden omschreven, en van artikel 38, lid 2, waarbij de verwerkingsverantwoordelijke opgedragen wordt aan de functionaris voor gegevensbescherming "de benodigde middelen […] voor het vervullen van deze taken" ter beschikking te stellen, wat ook de tijd omvat die hij nodig heeft om zich van deze taken te kwijten. De samensmelting van de functie van veiligheidsconsulent en van functionaris voor gegevensbescherming tot een door één enkel persoon uit te oefenen functie, dreigt afbreuk te doen aan die vereisten.

Artikel 10 en artikel 49, a), moeten herzien worden in het licht van deze opmerking.

Artikel 12

1. Bij het ontworpen artikel 5*bis* van de wet van 15 januari 1990 worden bepaalde bestuursdiensten gemachtigd om, "hetzij elk voor zich, hetzij gezamenlijk, in uitvoering van hun respectieve wettelijke opdrachten […] persoonsgegevens [te] verzamelen, [te] verwerken en samen [te] voegen met het oog op de oprichting van een *datawarehouse* waarmee ze enerzijds in staat worden gesteld om gerichte controles uit te voeren op basis van risico-indicatoren en anderzijds analyses kunnen uitvoeren op relationele gegevens afkomstig van verschillende instanties".

De afdeling Wetgeving verstaat daaronder dat bij die bepaling talrijke vormen van gegevensverwerking ingesteld worden: het aanmaken van een *datawarehouse*, de verzameling van (niet in de tekst bepaalde) gegevens door de genoemde instellingen, de input en de samenvoeging van die gegevens in dat zogeheten "*datawarehouse*", de toepassing van "antifraude-algoritmen" op de in het "*datawarehouse*" opgeslagen gegevens, de toepassing van een profileringstechniek om een verband te kunnen leggen tussen de verwerkte gegevens en frauderisico-indicatoren, het gebruik van die gegevens bij het nemen van een bestuurlijke

‡LW-BGFSMBJEA-GDCACUQ‡

beslissing met betrekking tot de controle van de betrokken personen en, bovendien, het gebruik van die gegevens voor analyse.

Die bepaling geeft aanleiding tot de hiernavolgende punten van kritiek ten aanzien van artikel 8 van het Europees Verdrag voor de rechten van de mens en van artikel 22 van de Grondwet, inzonderheid van de daarin vervatte vereisten inzake wettelijkheid en voorzienbaarheid, alsook van de artikelen 6, lid 3, en 22 van de AVG.

Het wettelijkheidsvereiste houdt inzonderheid in dat de toelaatbaarheidsvoorwaarden met betrekking tot de verwerking van persoonsgegevens door de wetgever moeten worden bepaald en niet door de administratie zelf: als de regeling inzake de gegevensverwerking aan de administraties zelf overgelaten zou worden, zouden die administraties geneigd kunnen zijn de noodzaak van dergelijke verwerkingen voornamelijk te beoordelen op grond van hun onmiddellijk belang, namelijk efficiënt bestuur, en te weinig gewicht te geven aan de bescherming van de persoonlijke levenssfeer van de burgers.

2. Bij artikel 22 van de Grondwet is de wetgever eveneens verplicht wetten uit te vaardigen die toegankelijk en begrijpelijk zijn,[20] een vereiste dat, zoals hierboven in herinnering wordt gebracht, terugkomt in de rechtspraak van het Grondwettelijk Hof.

Bovenop het feit dat dergelijke duidelijkheid eenieder de mogelijkheid moet bieden om te weten welke gevolgen de wet aan zijn handelingen verbindt, is een duidelijke wetgeving uitermate belangrijk in het kader van e-government, teneinde het optreden van de uitvoerende macht af te bakenen en machtsmisbruik te voorkomen en te controleren. Daarom moet eenieder "de omvang en de voorwaarden voor de uitoefening van de beoordelingsbevoegdheid van de overheden op het betrokken terrein" kennen.[21]

Zoals de Commissie voor de bescherming van de persoonlijke levenssfeer daar in haar advies aan heeft herinnerd,[22] betekent dit concreet dat de wetgever de essentiële elementen van de georganiseerde verwerkingen van persoonsgegevens moet bepalen, zoals dat blijkt uit de rechtspraak van het Grondwettelijk Hof en van de afdeling Wetgeving van de Raad van State.

[20] Zie inz. EHRM 2 augustus 1984, *Malone t. Verenigd Koninkrijk*, § 67. Die waarborgen zijn toegepast op de gegevensverwerkingen in arrest *Rotaru t. Roemenië* van 4 mei 2000, § 52 en § 55, van het Europees Hof voor de Rechten van de Mens.

[21] Zie inz. EHRM 16 februari 2000, *Amann t. Zwitserland*, § 62.

[22] Advies 34/2018 van 11 april 2018 over het voorontwerp waarover dit advies gegeven wordt. Wanneer in dit advies verwezen wordt naar het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, wordt dat advies 34/2018 bedoeld.

‡LW-BGFSMBJEA-GDCACUQ‡

In het bijzonder moet de wetgever, voor elke gegevensverwerking, zelf de categorieën gegevens die gebruikt worden alsook de wijze waarop die gegevens verzameld worden, vaststellen.[23]

Het doeleinde dat met de verwerking wordt nagestreefd, in de Franse tekst ook "finalité" genoemd, is een essentieel element van de verwerking.[24]

Hetzelfde geldt voor de bewaartermijn van de gegevens. Dat veronderstelt dat de wetgever minstens de maximale bewaartermijnen voor de gegevens bepaalt.[25]

De wetgever moet eveneens de verwerkingsverantwoordelijke aanduiden.[26]

De mededeling van de informatie, ook het "hergebruik" genoemd, moet eveneens door de wetgever zelf geregeld worden.[27]

---

[23] Advies 37.765/1/2/3/4, op 4 november 2004 verstrekt over een voorontwerp dat ontstaan gegeven heeft aan de programmawet van 27 december 2004, *Parl.St.* Kamer 2004-05, nr. 1437, 634; advies 41.662/1/2/3/4, op 14, 16 en 17 november 2006 verstrekt over een voorontwerp van wet dat ontstaan gegeven heeft aan de programmawet (I) van 27 december 2006, *Parl.St.* Kamer 2006-07, nr. 2773/1, 425; advies 40.079/2, op 12 april 2006 verstrekt over een voorontwerp dat ontstaan gegeven heeft aan de wet van 28 december 2006 'houdende instemming met het verdrag tussen het Koninkrijk België, de Bondsrepubliek Duitsland, het Koninkrijk Spanje, de Republiek Frankrijk, het Groothertogdom Luxemburg, het Koninkrijk der Nederlanden en de Republiek Oostenrijk inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van het terrorisme, de grensoverschrijdende criminaliteit en de illegale migratie, en met de bijlagen, gedaan te Prüm op 27 mei 2005', *Parl.St.* Kamer 2005-06, nr. 2645/1; advies 27.289/4, op 25 februari 1998 verstrekt over een voorontwerp dat ontstaan gegeven heeft aan de wet van 21 december 1998 'betreffende de veiligheid bij voetbalwedstrijden', *Parl.St.* Kamer 1997-98, nr. 1572/1, 50; adviezen 42.774/3 en 42.775/3, op 24 april 2007 verstrekt over een ontwerp van koninklijk besluit dat geleid heeft tot de wet van 21 augustus 2008 'houdende oprichting en organisatie van het eHealth-platform' (42.774/3) en een ontwerp van koninklijk besluit dat geleid heeft tot de wet van 21 augustus 2008 (nieuw opschrift) 'houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen' (42.775/3); advies 47.162/4, op 2 december 2009 verstrekt over een voorontwerp dat geleid heeft tot de wet van 19 mei 2010 'houdende oprichting van de Kruispuntbank van de voertuigen', *Parl.St.* Kamer 2009-10, nr. 52-2493/1, 38 tot 48.

[24] GwH 14 februari 2008, nr. 15/2008, B.22; 18 maart 2010, nr. 29/2010, B.11 en volg.; 13 januari 2011, nr. 1/2011, B.12.1 en volg.; advies 41.662/1/2/3/4, op 14, 16 en 17 november 2006 verstrekt over een voorontwerp dat ontstaan gegeven heeft aan de programmawet (I) van 27 december 2006, *Parl.St.* Kamer 2006-07, nr. 2773/1, 425; advies 38.782/2/V, op 11 augustus 2005 verstrekt over een voorontwerp dat geleid heeft tot de wet van 10 juli 2006 'betreffende de analyse van de dreiging', *Parl.St.* Kamer 2005-06, nr. 2032/1, 64.

[25] Adviezen 37.748/AV en 37.749/AV, op 23 november 2004 verstrekt over een voorontwerp dat geleid heeft tot de wet van 3 mei 2005 'houdende wijziging van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen' (37.748/AV) en over een voorontwerp dat geleid heeft tot de wet van 3 mei 2005 'houdende wijziging van de wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen' (37.749/AV), *Parl.St.* Kamer 2004-05, nrs. 1598/1 en 1599/1.

[26] Commissie voor de bescherming van de persoonlijke levenssfeer, advies 23/2008 van 11 juni 2008 betreffende een voorontwerp van wet 'houdende oprichting van de authentieke bron van voertuiggegevens', nr. 49; advies 42/2006, op 18 oktober 2006 gegeven over een voorontwerp van wet 'houdende de oprichting van een authentieke bron van voertuiggegevens', nr. 11.

[27] Advies 27.289/4, op 25 februari 1998 verstrekt over een voorontwerp dat geleid heeft tot de wet van 21 december 1998 'betreffende de veiligheid bij voetbalwedstrijden', *Parl.St.* Kamer 1997-98, nr. 1572/1, 50; advies 29.125/4, op 14 april 1999 verstrekt over een ontwerp dat geleid heeft tot het koninklijk besluit van 3 juni 1999 'houdende de regels voor het ticketbeheer ter gelegenheid van voetbalwedstrijden'; advies 37.765/1/2/3/4, op 4 november 2004 verstrekt over een voorontwerp dat geleid heeft tot de programmawet van 27 december 2004, *Parl.St.* Kamer 2004-05, nr. 1437; advies 43.186/3, op 19 juni 2007 verstrekt over een voorontwerp dat geleid heeft tot het decreet van 19 mei 2008 'over de Jeugdbijstand en houdende omzetting van maatregelen inzake jeugdbescherming', *Parl.St.* D.Parl. 2007-08, nr. 120/1; advies 43.489/4, op 10 december 2007 verstrekt over een voorontwerp dat geleid heeft tot het decreet van 30 april 2009 'betreffende de informatie, de coördinatie en de organisatie van de werven onder, op of boven de wegen of waterlopen', *Parl.St.* W.Parl. 2008-09,

‡LW-BGFSMBJEA-GDCACUQ‡

De wetgever moet bovendien de personen of instellingen vermelden die gemachtigd zijn om een gegevensbank te raadplegen.[28]

In lijn met die vereisten bepaalt artikel 6, lid 3, van de AVG dat voor de verwerkingen die uitgevoerd worden in de openbare sector de rechtsgrond vastgesteld wordt bij "lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is". En verder dat het "doel van de verwerking […] in die rechtsgrond vastgesteld" wordt, waarbij die rechtsgrond "specifieke bepalingen [kan] bevatten om de toepassing van de regels van deze verordening aan te passen, met inbegrip van […] de types verwerkte gegevens; de betrokkenen; de entiteiten waaraan en de doeleinden waarvoor de persoonsgegevens mogen worden verstrekt; de doelbinding; de opslagperioden; en de verwerkingsactiviteiten en -procedures, waaronder maatregelen om te zorgen voor een rechtmatige en behoorlijke verwerking […]".

3. Artikel 12 van het voorontwerp is te vaag om tegemoet te komen aan die vereisten.

De verwerkingen van persoonsgegevens waarvan sprake in die bepaling worden niet altijd omschreven, zelfs niet de essentiële elementen ervan, en wanneer dat wel gebeurt, is het op onduidelijke wijze.

Zoals de Commissie voor de bescherming van de persoonlijke levenssfeer in haar advies heeft onderstreept, komt dat neer op het geven van een "blanco cheque" aan de administratie.

Het laat zich meer in het bijzonder raden dat meerdere gegevensverwerkingen worden geregeld, maar die worden niet duidelijk vermeld in het ontwerp. Zo wordt in het voorontwerp gewag gemaakt van de oprichting van een "*datawarehouse*", een Engelse term die niet gedefinieerd wordt zodat het niet duidelijk is om welke gegevensverwerkingen het gaat. In de bespreking van het artikel staat dat dit geschiedt "met het oog op *datamatching* en *datamining*" maar die, overigens niet gedefinieerde, termen komen niet voor in de ontworpen tekst.

De loutere vermelding dat de betrokken instellingen "persoonsgegevens [kunnen] verzamelen" volstaat niet om duidelijk vast te stellen welke categorieën gegevens verwerkt worden, noch om de relevantie en de noodzaak van die inzameling te toetsen aan de nagestreefde doeleinden.

De wijze waarop die gegevens worden verzameld, wordt evenmin bepaald. De vraag rijst specifiek waaruit die gegevens geput zullen worden. De tekst vermeldt de medewerking van verschillende instellingen maar uit de bespreking van de bepaling lijkt

---

nr. 913/1, 239; advies 42.034, op 24 janvier 2007 verstrekt over een voorontwerp van wet 'betreffende bepaalde verwerkingen van persoonsgegevens door de Federale Overheidsdienst Financiën', *Parl.St.* Kamer nr. 52-3064/1. In dat laatste advies staat dat de "enkele machtiging van het Sectoraal Comité" niet voldoende is om "de mededeling van persoonsgegevens door de FOD Financiën aan beroepen of aan buitenlandse staten" te regelen.

[28] Advies 43.186/3, op 19 juni 2007 verstrekt over een voorontwerp dat geleid heeft tot het decreet van 19 mei 2008 'over de Jeugdbijstand en houdende omzetting van maatregelen inzake jeugdbescherming', *Parl.St.* D.Parl. 2007-08, nr. 120/1; advies 43.489/4, op 10 december 2007 verstrekt over een voorontwerp dat geleid heeft tot het decreet van 30 april 2009 'betreffende de informatie, de coördinatie en de organisatie van de werven onder, op of boven de wegen of waterlopen', *Parl.St.* W.Parl. 2008-09, nr. 913/1.

‡LW-BGFSMBJEA-GDCACUQ‡

opgemaakt te kunnen worden dat niet uitsluitend de gegevens van die instellingen verwerkt zullen worden aangezien de gegevens gehaald kunnen worden "uit elke pertinente publieke of private gegevensbank, met inachtneming van de vereiste beraadslagingen".

In het ontworpen artikel 5*bis*, tweede lid, van de wet van 15 januari 1990 staat weliswaar dat de beraadslagingen van de bevoegde kamer van het informatieveiligheidscomité "de aard van de meegedeelde gegevens [bepalen]", maar die procedure vormt, hoewel ze niet overbodig is, geen wettelijke basis waarbij bepaald wordt welke gegevens verwerkt worden, zoals eveneens gesteld wordt in het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.

Er wordt niet bepaald welke doeleinden nagestreefd worden met de verschillende verwerkingen.

Voor het betreffende *datawarehouse* wordt geen enkele verwerkingsverantwoordelijke aangewezen.

Er wordt evenmin voorzien in een duidelijke regeling voor het hergebruik van de gegevens en de mededeling ervan aan dat *datawarehouse*. Hoe vaak zullen die gegevens hergebruikt worden? Valt dat hergebruik onder de opdrachten van de administratie die die gegevens meedeelt en van het *datawarehouse* dat ze ontvangt (en waarvan niet geweten is welk doeleinde het nastreeft)? Is het de bedoeling om gegevens te hergebruiken voor andere doeleinden dan die waarvoor ze verzameld zijn (bijvoorbeeld gegevens die aanvankelijk verzameld zijn met het oog op de toekenning van een uitkering of het beheer van een administratief dossier hergebruiken voor controles)?

In de voorliggende tekst wordt eveneens gebruikgemaakt van het begrip "risico-indicatoren", maar er wordt niet in vermeld waar het precies om gaat, noch wie die indicatoren definieert.

Er is eveneens sprake van "analyses". De vraag rijst wat die analyses gebaseerd op gegevensverwerkingen inhouden, wie ze uitvoert en met welk doel.

Wat de "relationele gegevens afkomstig van verschillende instanties" betreft, rijzen de volgende vragen: wat is een "relationeel gegeven", om welke "verschillende instanties" gaat het en welke doeleinden worden nagestreefd?

4. Het begrip "frauderisico-indicatoren", dat weliswaar niet gedefinieerd wordt in de tekst, doet denken aan het gebruik van de techniek van profilering, zoals eveneens vermeld wordt in het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.[29]

In artikel 4, 4) van de AVG wordt "profilering"als volgt gedefinieerd:

> "elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties,

[29] § 32.

‡LW-BGFSMBJEA-GDCACUQ‡

economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen".

Profilering houdt met andere woorden in dat de persoonsgegevens van de burger ingevoerd worden in een rekenprogramma dat onder meer gebruikt kan worden om vergelijkingen te maken en statistische verbanden te leggen. Op grond van het resultaat van die berekeningen wordt het individu tot een vooraf bepaalde bevolkingscategorie gerekend, die specifieke kenmerken vertoont die een grond vormen om ten aanzien van die categorie een bijzondere houding aan te nemen, zoals bijvoorbeeld een fiscale inspectie voor vermoedelijke fiscale fraudeurs.[30]

Uit artikel 22, lid 1, van de AVG blijkt dat het in principe verboden is een persoon te onderwerpen "aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft". Er wordt onder meer een uitzondering gemaakt op dat verbod wanneer het besluit, overeenkomstig artikel 22, lid 2, b), van dezelfde verordening, "is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene". Er valt ook op te merken dat een dergelijk besluit niet genomen kan worden over de gevoelige gegevens waarnaar in artikel 9, lid 1, van de AVG verwezen wordt, zelfs niet in het geval bedoeld in artikel 22, lid 2, b), behalve in het geval waarin artikel 9, lid 2, g), voorziet (de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang) en op voorwaarde dat "er passende maatregelen ter bescherming van de [rechten en vrijheden en de] gerechtvaardigde belangen van de betrokkene zijn getroffen".

Indien het effectief de bedoeling van de wetgever is om met de oprichting van een *datawarehouse* en door gebruik te maken van technieken van *datamatching* en *datamining* de techniek van profilering te gebruiken, moet in afdoende waarborgen voorzien worden.

Er dient bijzondere aandacht besteed te worden aan de rechten van de personen met betrekking tot wie een besluit genomen is dat steunt op de techniek van profilering. Gebruikmaken van profilering in de overheidssector houdt immers risico's in. De hoeveelheid gegevens afkomstig van alle administraties die verwerkt wordt is zodanig groot dat fouten onvermijdelijk zijn. Die fouten kunnen echter aanzienlijke gevolgen hebben, aangezien het individu voor wie een verkeerd profiel opgesteld wordt, tot een bevolkingscategorie gerekend zal worden waartoe hij in feite niet behoort. Hij zal dan ook, soms meermaals, te maken krijgen met discriminerende beslissingen waardoor hem ten onrechte goederen of diensten ontzegd worden

[30] M. HILDEBRANDT, "Who is Profiling Who? Invisible Visibility" in S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne en S. Nouwt (eds.), *Reinventing Data Protection?*, Dordrecht, Springer, 2009, 241; V. PAPAKONSTANTINOU, "A Data Protection Approach to Data Matching Operations Among Public Bodies", *International Journal of Law and Information Technology* 2001, vol. 9, nr. 1, pp. 62 en 63; J.-M. DINANT, C. LAZARO, Y. POULLET, N. LEFEVER en A. ROUVROY, "L'application de la Convention 108 au mécanisme de profilage. Eléments de réflexion destinés au travail futur du Comité consultatif", maart 2008, T-PD (2008) 01, 5.

‡LW-BGFSMBJEA-GDCACUQ‡

waarop hij zonder die fout wel recht had gehad.[31] Het Grondwettelijk Hof heeft trouwens onlangs het volgende in herinnering gebracht:

> "Het is (…) van groot belang dat bij die techniek de juiste selectiecriteria (geheel van karakteristieken) worden gebruikt om de strijd tegen sociale fraude te versterken (het zgn. fraudeknipperlicht of de zgn. risico-indicatoren). Er zijn immers, *a fortiori* in de beginfase van het opzet, ernstige gebreken verbonden aan die techniek, (…), hetgeen noopt tot een permanente opvolging en evaluatie van de criteria (zie Privacycommissie, advies 24/2015, p. 7; advies 05/2016, p. 6."[32]

en er het volgende aan toegevoegd:

> "Die verwerkingstechniek houdt (…) risico's (…) in doordat onder meer verkeerde verbanden tussen kenmerken van een bepaald gedrag en personen kunnen worden gelegd. Derhalve dient de wetgever te voorzien in voldoende waarborgen."[33],

hetgeen onder meer veronderstelt dat de verwerkingsverantwoordelijke bij wet aangewezen wordt, dat een proportionele verwerking ingevoerd wordt, dat de rechten van de betrokkenen en inzonderheid het recht op inzage van de gegevens in acht genomen worden zodra het niet langer nodig is dat recht te schorsen ten behoeve van een onderzoek, alsook dat in adequate rechtsmiddelen wordt voorzien.

Gelet op het risico dat er fouten gemaakt worden bij de profilering van een betrokken persoon, zou inzonderheid het recht op beperking van de verwerking toegepast moeten worden, omdat een persoon die verkeerd geprofileerd zou worden op grond van dat recht de verwerking kan verhinderen totdat die fout rechtgezet wordt. Dat recht is verankerd in artikel 18 van de AVG. Het ontworpen artikel 5*quater* van de wet van 15 januari 1990 wijkt echter af van dat artikel 18 "wanneer en voor zover sociale gegevens van persoonlijke aard verwerkt worden".[34]

5. Kortom, er kan niet van uitgegaan worden dat de oprichting van een *datawarehouse* dat een groot aantal gegevens verwerkt en waarbij een groot deel van de burgers of zelfs alle burgers betrokken zijn en dat eventueel gebruikmaakt van technieken van profilering onschuldig is. De oprichting ervan moet dan ook op zijn minst gepaard gaan met de begeleidende maatregelen waarvan sprake is in de voorgaande opmerkingen.

Artikel 13

De bewoordingen van het ontworpen artikel 5*ter* van de wet van 15 januari 1990 beantwoorden niet aan de vereisten van wettelijkheid en voorzienbaarheid.

[31] Aanbeveling CM/Rec(2010)13 van het Comité van ministers aan de lidstaten 'over de bescherming van personen met betrekking tot de automatische verwerking van persoonsgegevens in het kader *van profilering*', 23 november 2010. Zie eveneens punt 72 van de memorie van toelichting bij die aanbeveling.

[32] GwH 15 maart 2018, nr. 29/2018, B.3.5.

[33] *Ibid.*, B.31.

[34] Er wordt eveneens verwezen naar de opmerking gemaakt bij artikel 14.

‡LW-BGFSMBJEA-GDCACUQ‡

Het gaat in het bijzonder om de woorden "elk persoonsgegeven", "uitvoering van hun wettelijke opdrachten" en "in het kader van een andere wettelijke opdracht". Het zou kunnen gaan om een verdere verwerking die onverenigbaar is met de doeleinden die bij het verzamelen van de gegevens worden nagestreefd, hetgeen verboden is bij artikel 5, lid 1, b), van de AVG. Zoals gesteld wordt in overweging 50 van de AVG:

> "[kan] [i]ndien de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend, (…) in het Unierecht of het lidstatelijke recht worden vastgesteld en gespecificeerd voor welke taken en doeleinden de verdere verwerking als rechtmatig en verenigbaar met de aanvankelijke doeleinden moet worden beschouwd."

Die preciseringen ontbreken *in casu*.

Artikel 14

De bewoordingen van het ontworpen artikel 5*quater* van de wet van 15 januari 1990 beantwoorden niet aan de vereisten van wettelijkheid en voorzienbaarheid.

De bepaling wijkt af van het recht op beperking van de verwerking maar vermeldt niet om welke gevallen het gaat.

Voorts is ook niet duidelijk op welke categorieën van gegevens die beperking betrekking heeft, aangezien de opsomming van die categorieën in de tekst voorafgegaan wordt door de woorden "in het bijzonder".

Artikel 19

In het ontworpen artikel 15, § 1, tweede zin, van de wet van 15 januari 1990 wordt niet gepreciseerd welke criteria de machtiging die aan de Koning verleend wordt afbakenen.

De ontworpen paragraaf 2, zesde lid, voorziet in een uitzondering op de verplichting om de machtiging van het comité te verkrijgen. De steller van het voorontwerp moet die uitzondering kunnen rechtvaardigen.

Wat betreft de ontworpen paragraaf 3, verbaast de afdeling Wetgeving zich over het feit dat het comité bevoegd is om zich uit te spreken over het gebruik van het identificatienummer van het Rijksregister, terwijl dit een persoonsgegeven is dat uitgaat van een authentieke bron, namelijk het "Rijksregister" waarvoor de FOD Binnenlandse Zaken verantwoordelijk is.

‡LW-BGFSMBJEA-GDCACUQ‡

Artikel 40

In de veronderstelling dat de steller van het voorontwerp de kamer "sociale zekerheid en gezondheid" opvat als een onafhankelijke administratieve overheid[35], dient over het ontworpen artikel 46 van de wet van 15 januari 1990 de volgende opmerking te worden gemaakt.

In advies nr. 42.387/VR van 27 maart 2007 heeft de afdeling Wetgeving het volgende in herinnering gebracht:

> "[...] met betrekking tot het toekennen van een bevoegdheid van verordenende aard aan een overheid die niet politiek verantwoordelijk is, [heeft] de Raad van State, afdeling wetgeving, in het verleden er al meermaals (...) op gewezen dat het toekennen van reglementaire bevoegdheid aan openbare instellingen of organen ervan, moeilijk in overeenstemming te brengen valt met de algemene principes van het Belgisch publiek recht, aangezien erdoor wordt geraakt aan het beginsel van de eenheid van de verordenende macht en terzake iedere rechtstreekse parlementaire controle ontbreekt. Verordeningen van die aard ontberen daarenboven de waarborgen waarmee de klassieke regelgeving gepaard gaat, zoals die inzake de bekendmaking en de preventieve controle van de afdeling wetgeving van de Raad van State.
>
> Als er in het verleden al uitzonderingen op het delegatieverbod van reglementaire bevoegdheid aan openbare instellingen toelaatbaar werden geacht door de Raad van State, afdeling wetgeving, betrof het doorgaans delegaties met een beperkte draagwijdte en van een zodanig technische aard, dat ervan mocht worden uitgegaan dat de instellingen die de betrokken reglementering dienden toe te passen, ook het best geplaatst waren om deze met kennis van zaken uit te werken en de aldus gedelegeerde bevoegdheid uit te oefenen"[36].

De aanvaardbaarheid van een delegatie van verordenende bevoegdheid aan een onafhankelijke administratieve overheid is dus[37] gekoppeld aan beperkende voorwaarden. Onder andere[38] in advies 44.607/1 van 12 juni 2008[39], is in dat verband gesteld dat[40]:

> "de decreetgever in beginsel enkel aan de regering normatieve bevoegdheden vermag te verlenen, omdat uitgesloten is dat de verordenende macht wordt uitgeoefend op een andere wijze dan is voorgeschreven door de Grondwet.

---

[35] In dat verband wordt verwezen naar algemene opmerking D.

[36] Advies 42.387/VR van 27 maart 2007 over een voorontwerp dat geleid heeft tot de wet van 15 mei 2007 'houdende instemming met het samenwerkingsakkoord tussen de Federale Overheid, het Vlaams Gewest, het Waals Gewest en het Brussels Hoofdstedelijk Gewest inzake de uitvoering van sommige bepalingen van het Protocol van Kyoto, afgesloten te Brussel, op 19 februari 2007', *Parl.St.* Senaat 2006-07, nr. 3-2411/1, 34.

[37] Zonder dat hier de kwestie ter sprake gebracht moet worden van de weerslag die het bestaan van verplichtingen voortvloeiend uit het afgeleid recht van de Europese Unie op die aanvaardbaarheid zou kunnen hebben (zie in dat verband advies 50.003/4 op 26 september 2011 gegeven over een voorontwerp dat ontstaan heeft gegeven aan de wet van 10 juli 2012 'houdende diverse bepalingen inzake elektronische communicatie').

[38] Zie ook advies nr. 50.217/4 gegeven op 21 september 2011 over een ontwerp dat ontstaan gegeven heeft aan het koninklijk besluit van 2 december 2011 'betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer'.

[39] Advies nr. 44.607/1 gegeven op 12 juni 2008 over een voorontwerp dat geleid heeft tot het decreet van 10 juli 2008 'betreffende het stelsel van leren en werken in de Vlaamse Gemeenschap', *Parl.St.* Vl. Parl. 2007-08, nr. 1760/1, 241 tot 265.

[40] Zie eveneens J. VANDE LANOTTE, G. GOEDERTIER, Y. HAECK, J. GOOSSENS en T. DE PELSMAEKER, *Belgisch Publiekrecht*, vol. 1, Brugge, Die Keure, 2015, 148 en 149.

‡LW-BGFSMBJEA-GDCACUQ‡

> Deze grondwettelijke regels betekenen niet dat er geen enkele ruimte zou zijn voor een medewerking van andere instanties bij de verordenende bevoegdheid. Evenwel mogen daarbij de grondwettelijke regels betreffende de uitoefening van de normatieve functie niet worden miskend. Het grondwettigheidsbezwaar tegen het laten vaststellen van regels door instanties die geen politieke verantwoordelijkheid dragen, worden opgevangen wanneer aan het uitvoerend orgaan ten aanzien van die regels een goedkeuringsbevoegdheid wordt toegekend die zo is opgevat dat geen afbreuk wordt gedaan aan de genoemde grondwettelijke regels; daarenboven mag het aangewende procédé er niet toe leiden dat de regering wordt belemmerd in de uitoefening van de haar toekomende prerogatieven op normatief vlak […]. Een zulkdanige fragmentering van de verordeningsmacht van het uitvoerend orgaan, die er op neerkomt dat de regering het initiatiefrecht en ook de vrije appreciatie van de maatregelen die nodig zijn voor de uitvoering van het decreet ontnomen wordt, is in strijd met artikel 33 van de Grondwet".

Het ontworpen artikel 46, § 2, van de wet van 15 januari 1990 bepaalt dat de beraadslagingen van het informatieveiligheidscomité "een algemene bindende draagwijdte jegens derden [hebben]" en dat deze niet in strijd mogen zijn met hogere rechtsnormen. In de memorie van toelichting staat daaromtrent te lezen:

> "De beraadslagingen van het Comité hebben een normatieve waarde (wet in materiële zin), overeenkomstig de grondwettelijke bepalingen en kunnen worden betwist volgens de geldende rechtsmiddelen indien ze tegenstrijdig zijn met hogere juridische normen".

Een dergelijke delegatie van verordenende bevoegdheid druist in tegen de hiervoor vernoemde aanvaardbaarheidsvoorwaarden, zowel wegens de omvang ervan, als wegens het feit dat de rechtsregels die het resultaat zijn van de uitvoering van die delegatie van bevoegdheid niet door een politiek verantwoordelijke overheid worden bekrachtigd.

Het ontworpen artikel 46, § 2, van de wet van 15 januari 1990 moet grondig worden herzien in het licht van die opmerking.

Dezelfde opmerking geldt voor het ontworpen artikel 35/1, § 1, van de wet van 15 augustus 2012 (artikel 80 van het voorontwerp).

Artikel 47

Hoewel het begrijpelijk was dat het thans geldende artikel 6 van de wet van 21 augustus 2008 'houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen' voorbehoud maakt voor de toepasbaarheid van de wet van 8 december 1992, is zulk een voorzorgsmaatregel niet meer noodzakelijk wat betreft de rechtens opgelegde toepasbaarheid van de AVG.

De verwijzing naar die verordening dient uit het ontworpen artikel 6 van de wet van 21 augustus 2008 te worden geschrapt zodat het voorbehoud alleen nog geldt voor de wet van 22 augustus 2002 'betreffende de rechten van de patiënt' en "de wettelijke en reglementaire bepalingen met betrekking tot de uitoefening van de geneeskunde".

‡LW-BGFSMBJEA-GDCACUQ‡

Artikelen 60 tot 68

1. De artikelen 60 tot 68 van het voorontwerp beogen uitvoering te geven aan artikel 23 van de AVG, dat de lidstaten machtigt de reikwijdte te beperken van de rechten en verplichtingen van de betrokkenen waarin de AVG voorziet.

De lidstaat heeft in dat verband de verplichting om specifieke bepalingen uit te vaardigen met betrekking tot de verschillende punten die opgesomd worden in artikel 23, lid 2, van de AVG.

Artikel 23, lid, 2, f), van de AVG voorziet in de verplichting om specifieke maatregelen te nemen met betrekking tot "de opslagperiodes en de toepasselijke waarborgen, rekening houdend met de aard, de omvang en de doeleinden van de verwerking of van de categorieën van verwerking".

Het dispositief moet in die zin aangevuld worden.

2. In de ontworpen artikelen 100/14, § 3, zesde lid, 100/15, § 3, zesde lid, 100/13, § 3, zesde lid, en 100/17, § 3, zesde lid, van het Sociaal Strafwetboek (artikelen 62, 64, 66 en 67 van het voorontwerp) moet meer in het algemeen verwezen worden naar het geheel van de actiemogelijkheden van het openbaar ministerie.

3. Dezelfde opmerkingen gelden *mutatis mutandis* voor de artikelen 71 tot 79 van het voorontwerp.

Artikelen 71 tot 79

Voor de federale overheidsdienst Financiën wordt de afwijkende regeling wat betreft de rechten van de betrokkenen inzake het privéleven, thans geregeld bij artikel 3, § 7, van de wet van 8 december 1992.

Die bepaling voorziet in slechts één afwijking op artikel 10 (recht op toegang) van de wet van 8 december 1992. Er wordt in geen enkele afwijking voorzien op artikel 9 (recht op informatie) of op artikel 12 (recht op rectificatie).

De steller van het voorontwerp moet dan ook kunnen rechtvaardigen dat zulke mogelijkheden tot afwijking voortaan noodzakelijk zijn.

Artikelen 82 en 83

De artikelen 82 en 83 van het voorontwerp beogen uitvoering te geven aan artikel 23 van de AVG, dat de lidstaten machtigt de reikwijdte te beperken van de rechten en verplichtingen van de betrokkenen waarin de AVG voorziet.

‡LW-BGFSMBJEA-GDCACUQ‡

Zoals blijkt uit het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, voorziet het ontworpen artikel XV.10/1 van het Wetboek van economisch recht (artikel 82 van het voorontwerp) in een bijzonder ruime beperking van de rechten van de betrokkene. Alle rechten vermeld in hoofdstuk III "Rechten van de betrokkene" (artikelen 12 tot 22 van de AVG alsook artikel 34 van die AVG, betreffende de "mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene") worden immers noodzakelijkerwijs systematisch uitgesloten wanneer de inspectiediensten en / of de controlediensten waarvan de bevoegdheden vastgesteld worden in het Wetboek van economisch recht, persoonsgegevens verwerken.

Artikel 23 van de AVG maakt het weliswaar mogelijk dat de reikwijdte van de rechten bepaald bij de artikelen 12 tot 22 en 34 van de AVG wordt beperkt, maar schrijft ook voor dat de lidstaat daartoe het bewijs levert van een gerechtvaardigd doel, in de zin van artikel 23, lid 1, van de AVG, dat "die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel is". Die bepaling moet trouwens strikt worden geïnterpreteerd, aangezien ze een afwijkende bepaling is.

Een overheidsinmenging in het recht op eerbiediging van het privéleven dient niet alleen te steunen op een voldoende precieze wettelijke bepaling, ze dient daarenboven op een redelijke verantwoording te berusten en evenredig te zijn met de doelstellingen die nagestreefd worden door de wetgever, die ter zake over een appreciatiemarge beschikt. Die appreciatiemarge is evenwel niet onbegrensd: opdat een wettelijke regeling verenigbaar is met het recht op eerbiediging van het privéleven, is vereist dat de wetgever een billijk evenwicht heeft gevonden tussen alle rechten en belangen die in het geding zijn.

De uitoefening van de rechten waarin de artikelen 12 tot 22 en 34 van de AVG voorzien, draagt bij tot een dergelijk evenwicht, gelet op de inmengingen in het recht op eerbiediging van het privéleven die de AVG en de ontworpen wet toestaan.

Door noodzakelijkerwijs systematisch te voorzien in de volledige uitsluiting(2) van alle(3) rechten bedoeld in de artikelen 12 tot 22 en 34 van de AVG voor bepaalde categoriën van verwerkingen – en onrechtstreeks ook voor bepaalde categorieën van verwerkingsverantwoordelijken – die zeer ruim omschreven zijn(4), zelfs zonder dat de inspectiedienst of de controledienst het bewijs moeten leveren dat zulk een uitsluiting noodzakelijk is opdat zij hun taken naar behoren kunnen vervullen(1), voldoet de wetgever niet aan de evenredigheidsvereiste waaraan hij zich dient te houden.

Artikel 82 van het voorontwerp is te ruim gesteld om een passende afweging van de bestaande rechten mogelijk te maken opdat de rechten van de betrokkenen niet meer worden ingeperkt dan wat strikt noodzakelijk is voor de realisatie van het nagestreefde gerechtvaardigde doel.

‡LW-BGFSMBJEA-GDCACUQ‡

Artikel 86

Artikel 86 strekt ertoe om met betrekking tot de rol van de huidige sectorale comités van de Commissie voor de bescherming van de persoonlijke levenssfeer, te zorgen voor de overgang tussen het huidige geldende recht en het recht dat zal voortvloeien uit de aanneming van de wet waarvan het voorontwerp thans ter fine van advies is voorgelegd.

Er dient evenwel rekening te worden gehouden met het feit dat de kaderwet, zoals het voorontwerp ervan alvast is opgevat, in het verlengde van de AVG, in principe het vergunningssysteem vervangt door een responsabiliseringsmechanisme.

Met het voorliggende voorontwerp wordt weliswaar het systeem opnieuw ingevoerd waarbij voorzien wordt in een vergunning door de kamer "sociale zekerheid en gezondheid" of de kamer "federale overheid" van het comité, in ieder geval wat betreft de uitwisseling van gegevens waarvan sprake in verschillende ontworpen bepalingen. Dat neemt evenwel niet weg dat de wil van de wetgever, zoals die blijkt uit de teksten die hij zal aannemen, op voorwaarde dat deze niet gewijzigd worden ten opzichte van het voorontwerp van kaderwet en van het voorontwerp, niet voldoende duidelijk tot uiting zal komen wat betreft zijn visie op de rol van de instanties die in de plaats moeten komen van de sectorale comités; op dat vlak wordt verwezen naar algemene opmerking B.

Het staat aan de wetgever zelf om, met name wat betreft de huidige rol van de sectorale comités, te zorgen voor de overgang tussen het huidige recht en het recht in wording. Hij mag dat niet overlaten aan de adressaten van de wetten die thans worden voorbereid, volgens de interpretatie die zij daarvan geven, aangezien de grondslagen voor de mogelijke interpretaties te vaag zijn.

Artikel 87

Artikel 87 van het voorontwerp strekt ertoe de Koning een machtiging te verlenen op grond waarvan Hij

> "de bestaande wettelijke bepalingen [kan] wijzigen, aanvullen, vervangen of opheffen om de tekst ervan in overeenstemming te brengen met de bepalingen van deze wet".

In de bespreking van dat artikel wordt enkel gesteld dat deze bepaling

> "de Koning de bevoegdheid [geeft] om eventuele wettelijke bepalingen die niet in overeenstemming zijn met deze wet aan te passen. Deze aanpassingen kunnen geen betrekking hebben op de privacykaderwet".

‡LW-BGFSMBJEA-GDCACUQ‡

Het spreekt vanzelf dat de aldus beoogde machtiging, gelet inzonderheid op het legaliteitsbeginsel dat voortvloeit uit artikel 22 van de Grondwet, hoe ruim de invulling ervan ook is, enkel betrekking mag hebben op de vormelijke en wetgevingstechnische uitvoering van de keuzes die gemaakt zijn in het voorliggende voorontwerp van wet. Die machtiging mag er niet toe leiden dat de Koning de bevoegdheid wordt verleend om zelf nieuwe inhoudelijke keuzes te maken inzake de regeling van deze aangelegenheid.

LE GREFFIER – DE GRIFFIER LE PRÉSIDENT – DE VOORZITTER

Béatrice DRAPIER Pierre VANDERNOOT

‡LW-BGFSMBJEA-GDCACUQ‡