Avis n° 34/2018 du 11 avril 2018

Objet : demande d'avis concernant 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* (CO-A-2018-017)

La Commission de la protection de la vie privée (ci-après "la Commission") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après "la LVP"), en particulier l'article 29 ;

Vu la demande d'avis de Madame Maggie De Block, Ministre des Affaires sociales et de la Santé publique, reçue le 23/02/2018 ;

Vu la nouvelle version retravaillée de l'avant-projet de loi susmentionné, reçue le 16/03/2018 ;

Vu le rapport de Monsieur Dirk Van Der Kelen ;

Émet, le 11/04/2018, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS

1. La Ministre des Affaires sociales et de la Santé publique (ci-après le demandeur) sollicite l'avis de la Commission concernant 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* (ci-après l'avant-projet de loi).

2. L'avant-projet de loi doit exécuter sur plusieurs points le Règlement (UE) 2016/679 susmentionné du 27 avril 2016 (ci-après Règlement général sur la protection des données ou RGPD).

3. Dans un premier temps, l'avant-projet de loi souhaite créer un Comité de sécurité de l'information, qui doit compenser la disparition des comités sectoriels au sein de la Commission, à la suite de la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*.

4. L'avant-projet de loi entend ensuite fournir une base légale pour la création, par les institutions de sécurité sociale et les services d'inspection sociale, d'un datawarehouse à des fins de datamatching et de datamining, qui doit permettre de réaliser des contrôles et des analyses ciblés - dans le cadre de la lutte contre la fraude sociale.

5. Enfin, l'avant-projet de loi veut offrir à plusieurs services de contrôle et d'inspection dans les secteurs social, financier et économique la possibilité de limiter un certain nombre de droits dont disposent généralement les personnes concernées dans le cadre de la protection de leurs données à caractère personnel, et ce en application de l'article 23 du RGPD.

II. EXAMEN DE LA DEMANDE D'AVIS

1. INSTITUTION D'UN COMITÉ DE SÉCURITÉ DE L'INFORMATION

6. En application des articles 109 et suivants de la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, les comités sectoriels intégrés au sein de la Commission sont supprimés le 25 mai 2018.

7. L'avant-projet de loi crée dès lors un nouvel organe : le Comité de Sécurité de l'Information (ci-après CSI), constitué d'une chambre Sécurité Sociale et Santé (ci-après chambre SS&S)

et d'une chambre Autorité Fédérale (ci-après chambre AF), qui est chargé en particulier (mais pas exclusivement)[1] :

- de rendre des délibérations concernant certaines communications de données à caractère personnel[2] et
- de suivre la formation et le fonctionnement des délégués à la protection des données (ci-après DPO) des institutions de sécurité sociale et des institutions publiques et institutions de l'autorité fédérale.

1.1. Statut du CSI et de ses décisions

8. D'après l'Exposé des motifs de l'avant-projet de loi (p. 7), le CSI doit être considéré comme "*une mesure permettant de concrétiser les principes de base du GDPR en matière de 'privacy by design' et 'privacy by default'*".
   Ensuite, l'Exposé des motifs (p. 6) stipule aussi ce que le CSI n'est certainement pas :
   - il n'est pas une autorité de contrôle ;
   - il ne se substitue pas aux DPO respectifs ;
   - il n'est pas un responsable du traitement[3].

9. Dans ses délibérations, le CSI vérifiera de manière préventive si, lors des communications envisagées de données à caractère personnel, les conditions de limitation de la finalité, de proportionnalité et de sécurité définies dans le RGPD sont remplies (Exposé des motifs, p. 4).

10. La Commission constate donc que la création du CSI peut être perçue comme une mesure du législateur fédéral/de l'État belge visant à aider dans certains cas les responsables du traitement dans le secteur public à respecter leur responsabilité (articles 5.2 et 24 du RGPD). La Commission constate également que la possibilité d'une 'autorisation préalable' dans le chef de l'autorité de contrôle proprement dite, telle que prévue à l'article 36.5 du RGPD, est restée inexploitée. Elle souscrit toutefois à la plus-value de délibérations préalables concernant des communications de données à caractère personnel qui peuvent comporter certains risques pour les droits et libertés de la personne concernée, surtout dans le secteur de la sécurité sociale et de la santé. Elle constate en outre que le RGPD laisse au législateur

---

[1] Selon l'Exposé des motifs (p. 5), la chambre Sécurité Sociale et Santé peut (plus ou moins) être considérée comme le successeur du Comité sectoriel de la Sécurité Sociale et de la Santé et la chambre Autorité Fédérale reprend partiellement les compétences de l'actuel Comité sectoriel pour l'Autorité Fédérale (et du Comité sectoriel du Registre national).

[2] Pour la chambre SS&S, il s'agit principalement de communications de données sociales à caractère personnel ou de communications de données à caractère personnel relatives à la santé (voir l'article 40 de l'avant-projet de loi). Pour la chambre AF, il s'agit de communications de données à caractère personnel par des services publics fédéraux à des tiers (voir l'article 80 de l'avant-projet de loi). Pour certains flux de données, le CSI délibère en chambres réunies (voir les articles 19 et 80 de l'avant-projet de loi).

[4] Et ce par analogie avec ce qui est prévu pour le DPO/conseiller en sécurité de la plate-forme eHealth dans l'article 9, § 3 de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions*.

national la marge pour créer un tel organe, vu ses articles 6.2, 9.4 et 87. Elle renvoie également au considérant 41 du RGPD qui précise qu'une "mesure législative" ne doit pas nécessairement être une loi approuvée par un parlement. Dans cette optique, les délibérations du CSI peuvent, selon elle, également avoir un pouvoir normatif.

11. La Commission constate à cet égard que les articles 40 et 80 de l'avant-projet de loi prévoient explicitement que les délibérations émises par le CSI "*ont une portée générale contraignante envers les tiers*". La Commission reconnaît, comme cela a déjà été précisé, que les délibérations peuvent avoir un pouvoir normatif mais elle estime également que l'Autorité de protection des données (ci-après l'APD) doit pouvoir exercer librement les missions et les pouvoirs qui lui sont confiés (voir les articles 57 et 58 du RGPD) lors de l'évaluation d'un traitement de données à caractère personnel. Dans ce cadre, l'APD doit pouvoir agir en toute indépendance, libre de toute influence ou de toute instruction (voir l'article 52 du RGPD). Le RGPD n'autorise pas le législateur national à limiter le contrôle de l'APD pour les traitements de données à caractère personnel auxquels le RGPD s'applique.
Un problème peut survenir lorsque l'APD constate qu'une délibération du CSI est contraire à des normes juridiques supérieures. Dans ce cas, il est souhaitable que l'APD puisse le notifier de manière motivée au CSI et puisse demander une reconsidération de la délibération. Pour des raisons de sécurité juridique, cette demande n'a pas d'effet rétroactif.
Proposition de texte :
"L'Autorité de protection des données (APD) a le pouvoir de confronter les délibérations du CSI aux normes juridiques supérieures.
Sans préjudice de ses autres pouvoirs, l'APD, lorsqu'elle constate de manière motivée qu'une délibération n'est pas conforme à une norme juridique supérieure, peut inviter le CSI à reconsidérer la délibération dans les 45 jours sur les points qu'elle indique.
Une délibération ainsi reconsidérée doit alors être soumise à l'APD par le CSI dans les 30 jours précédant l'avis contraignant préalable."

Il est recommandé de reprendre également ce pouvoir dans le chef de l'APD dans la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, de sorte que l'ensemble de ses pouvoirs ne soit pas éparpillé dans plusieurs législations.

12. Par souci d'exhaustivité, la Commission attire également l'attention sur le fait qu'une délibération du CSI ne peut pas remplacer l'exécution d'une analyse d'impact relative à la protection des données, telle que visée à l'article 35 du RGPD, comme cela est d'ailleurs observé à juste titre en page 5 de l'Exposé des motifs.

13. La Commission souligne enfin que l'émission d'une délibération par le CSI pour le responsable du traitement concerné n'implique nullement une obligation de communiquer des données à caractère personnel. Ce dernier conserve à cet égard toute la liberté de juger lui-même de l'opportunité - comme cela est indiqué à juste titre dans l'Exposé des motifs (p. 14).

1.2. Formation et fonctionnement du délégué à la protection des données (DPO)

14. Une autre mission importante du CSI, prévue par l'avant-projet de loi (articles 40 et 80), en plus de rendre des délibérations en matière de flux de données, est celle de "*suivre si les délégués à la protection des données reçoivent la formation permanente adéquate et travaillent de façon coordonnée et, à défaut, prendre toutes mesures de soutien nécessaires pour assurer cette formation adéquate ou réaliser la coordination, notamment technique*".

15. La Commission présume que dans ce cadre, le CSI ne se substitue pas au responsable du traitement spécifique (ni au sous-traitant), qui, en vertu de l'article 38 du RGPD, ont pour mission :
    - d'associer le DPO, d'une manière appropriée et en temps utile, aux questions relatives à la protection des données à caractère personnel ;
    - d'aider le DPO et de lui fournir les ressources nécessaires pour exercer ses missions et lui permettre d'entretenir ses connaissances spécialisées.

    Afin d'exclure les malentendus à cet égard, la Commission propose de reformuler les dispositions citées comme suit : *"aider concrètement les délégués à la protection des données, en proposant entre autres une formation permanente adéquate et en formulant des recommandations, notamment au niveau technique"*.

16. La Commission fait par ailleurs remarquer que l'article 25 de l'avant-projet de loi permet d'également attribuer au DPO d'une institution de sécurité sociale, outre sa mission d'avis, "*l'exécution de missions qui lui sont confiées par la personne chargée de la gestion journalière*".

17. La Commission souhaite quand même rappeler en la matière que le DPO doit toujours pouvoir agir en toute indépendance. L'article 38.3 du RGPD prévoit explicitement que le responsable du traitement et le sous-traitant doivent veiller à ce que le DPO ne reçoive aucune instruction en ce qui concerne l'exercice de ses missions et l'article 38.6 du RGPD ajoute à cela que les missions qui lui sont confiées ne peuvent pas entraîner de conflit d'intérêts dans le chef du DPO.

18. La Commission recommande que l'avant-projet de loi souligne aussi explicitement l'indépendance du DPO. Concrètement, la Commission propose d'ajouter la formulation suivante : "*Dans la mesure où cela ne compromet pas l'indépendance du DPO et pour autant que le contenu et la quantité des autres missions qui lui sont confiées lui permettent de réaliser ses missions de DPO conformément au RGPD*".

19. La Commission estime également recommandé qu'une éventuelle intervention du Roi pour fixer les règles selon lesquelles le DPO d'une institution de sécurité sociale doit exercer des missions complémentaires (voir l'article 25, *in fine*, de l'avant-projet de loi) soit prévue après avis de l'APD[4].

20. Enfin, la Commission a encore des réserves quant à l'obligation reprise dans l'avant-projet de loi (voir les articles 10 et 24) dans le chef des institutions de sécurité sociale de communiquer l'identité du DPO à la chambre SS&S du CSI (en plus de la notification en la matière à la BCSS). En effet, l'article 37.7 du RGPD prévoit également déjà une communication de l'identité et des coordonnées des DPO à l'APD. Il est préférable d'éviter la surcharge administrative et le risque d'incohérences accompagnant une telle double obligation de notification.

1.3. Composition du CSI

21. La Commission estime que dans l'énumération des membres du CSI à l'article 2, § 2 de l'avant-projet de loi, il est préférable de commencer par les 2 membres qui font partie des deux chambres (c'est-à-dire les membres 1° et 4°), suivis des membres qui font partie d'une ou de l'autre chambre (c'est-à-dire les membres 2°, 3°, 5° et 6°).

22. Ensuite, la Commission considère également qu'à l'article 2, § 2, dernier alinéa de l'avant-projet de loi, il faut définir explicitement :
    - soit lequel des 2 membres visés à l'article 2, § 2, 5° et 6°, fait partie des chambres réunies,
    - soit que tous les membres des deux chambres font partie des chambres réunies.

23. La Commission estime qu'à l'article 3 de l'avant-projet de loi, il faut ajouter qu'un candidat ne peut pas non plus être membre du Gouvernement fédéral, d'un gouvernement communautaire ou régional, ni exercer une fonction dans une cellule stratégique d'un ministre.

---

[4] Et ce par analogie avec ce qui est prévu pour le DPO/conseiller en sécurité de la plate-forme eHealth dans l'article 9, § 3 de la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions*.

24. La Commission recommande qu'à l'article 6, § 1er de l'avant-projet de loi, il soit prévu qu'en cas d'empêchement du président, ce dernier soit remplacé par l'autre membre qui fait partie des deux chambres.

25. La 'requalification' aux articles 89 et 90 de l'avant-projet de loi des actuels présidents du Comité sectoriel de la Sécurité Sociale et de la Santé et du Comité sectoriel du Registre national en 'membres externes' est absurde. En effet, dans la mesure où l'actuelle Commission cesse d'exister le 25 mai 2018, il n'y aura plus, à ce moment-là, de membres 'internes'. Tous les actuels membres 'internes' (aussi bien les présidents que les membres 'internes' qui ne sont pas président) seront tous des membres 'externes' à partir du 25 mai 2018.

2. CRÉATION D'UN (DE) DATAWAREHOUSE(S) DANS LA LUTTE CONTRE LA FRAUDE SOCIALE

26. L'article 12 de l'avant-projet de loi entend créer une base légale générale pour les institutions de sécurité sociale, les services d'inspection sociale et la Direction des amendes administratives de la Division des études juridiques, de la documentation et du contentieux du SPF ETCS[5], soit pour ce qui les concerne respectivement, soit en commun, en exécution de leurs missions légales respectives, en vue de la création d'un (de) datawarehouse(s) à des fins de datamatching et de dataming, leur permettant d'effectuer des contrôles ciblés sur la base d'indicateurs de risques et de réaliser des analyses sur des données relationnelles des différentes institutions pour parvenir à une lutte efficace contre la fraude sociale.

27. Concernant les données à caractère personnel qui devront être regroupées dans le(s) datawarehouse(s), l'Exposé des motifs stipule que "*les données peuvent être puisées dans toute base de données pertinente, publique ou privée, dans le respect des délibérations requises*".

28. L'Exposé des motifs précise en outre que le CSI, conformément aux compétences qui lui sont attribuées, se prononcera sur les divers aspects de la communication de données à caractère personnel aux institutions de sécurité sociale et aux services d'inspection sociale et vérifiera en particulier si la communication de données à caractère personnel satisfait effectivement à la réglementation relative à la protection de la vie privée. On contrôlera ainsi si les principes

[5] Service public fédéral Emploi, Travail et Concertation sociale.

de finalité et de proportionnalité sont respectés et si lors du traitement, des mesures de sécurité suffisantes sont prévues.

29. L'article 12 de l'avant-projet de loi formule une finalité très large de 'datamatching et de datamining en vue d'une lutte efficace contre la fraude sociale[6]' pour la création d'un ou de plusieurs datawarehouse(s) dans lequel (lesquels) peuvent être regroupées des données (à caractère personnel) provenant de n'importe quelle base de données 'pertinente', publique ou privée. Une telle formulation large et globale offre en effet très peu de repères pour la personne concernée dont des données se retrouveront dans le(s) datawarehouse(s). Ni l'article 8 de la Convention européenne des droits de l'homme (ci-après la CEDH), ni l'article 22 de la Constitution, ni le RGPD, en particulier les articles 6.3 et 22, n'autorisent un tel 'chèque en blanc'.

30. Lorsque la base juridique d'un traitement de données à caractère personnel est une obligation légale ou sert une mission d'intérêt public, confiée au responsable du traitement, cette base juridique contient, conformément à l'article 6.3 du RGPD, plusieurs dispositions spécifiques concernant :
    - les types ou catégories 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 ;
    - les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal (on peut penser notamment à la pseudonymisation et au chiffrement).

    L'avant-projet de loi présente de graves manquements en la matière.

31. L'Exposé des motifs fait référence tant à l'article 8 de la CEDH, qu'à l'article 22 de la Constitution qui permettent une limitation du droit au respect de la vie privée (y compris la protection des données à caractère personnel) pour autant que cela soit prévu par la loi et aux conditions fixées par elle. Il va de soi que toute ingérence d'une autorité publique dans le droit au respect de la vie privée doit être prescrite dans une 'disposition légale suffisamment précise' qui répond à un besoin social impérieux et qui est proportionnelle à la finalité poursuivie.

[6] Il n'y a même aucune indication de tout ce qui est couvert par la 'fraude sociale'.

Une telle disposition légale précise doit définir les éléments essentiels des traitements de données à caractère personnel allant de pair avec l'ingérence de l'autorité publique[7]. Dans ce cadre, il s'agit :

- des finalités déterminées, explicites et légitimes ;
- des (catégories de) données à caractère personnel qui sont pertinentes et non excessives ;
- du délai de conservation maximal des données à caractère personnel enregistrées ;
- de la désignation du responsable du traitement.

32. En vertu de l'article 12 de l'avant-projet de loi, le datamining et le datamatching appliqués aux données à caractère personnel regroupées dans le datawarehouse (dont également 'des données sociales à caractère personnel relatives à la santé' telles que définies à l'article 9 de l'avant-projet de loi) doivent permettre d'effectuer des contrôles ciblés sur la base d'indicateurs de risques et de réaliser des analyses sur des données relationnelles des différentes institutions. Il peut donc être question d'une prise de décision individuelle automatisée, y compris le profilage.

33. La Commission rappelle dès lors l'article 22 du RGPD qui définit le principe selon lequel toute personne a le droit de ne pas faire l'objet d'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.
Une telle décision est toutefois possible, pour autant, notamment, qu'elle soit 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 libertés et des intérêts légitimes de la personne concernée.
Dans la mesure où, pour cette décision, des données sensibles sont utilisées au sens de l'article 9 du RGPD, le droit de l'Union ou le droit de l'État membre doit poursuivre un intérêt public important, garantir la proportionnalité de l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

[7] Voir DEGRAVE, E., "*L'e-gouvernement et la protection de la vie privée – Légalité, transparence et contrôle*", Collection du CRIDS, Larcier, Bruxelles, 2014, p. 161 e.s. (voir notamment : CEDH, arrêt *Rotaru c. Roumanie*, 4 mai 2000) ; Voir également plusieurs arrêts de la Cour constitutionnelle : l'arrêt n° 44/2015 du 23 avril 2015 (p. 63), l'arrêt n° 108/2017 du 5 octobre 2017 (p. 17) et l'arrêt n° 29/2018 du 15 mars 2018 (p. 26).

34. L'article 12 de l'avant-projet de loi présente également de graves manquements en la matière, vu l'absence de mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée[8].

35. La Commission fait enfin remarquer qu'une éventuelle délibération du CSI concernant certaines communications de données à caractère personnel qui iront de pair avec la gestion et l'exploitation du (des) datawarehouse(s) - bien qu'incontestablement utile - ne peut aucunement légitimer l'absence d'un document législatif de qualité[9] visant à encadrer un (de) tel(s) datawarehouse(s).

3. LIMITATIONS DES DROITS DES PERSONNES CONCERNÉES : Modifications

- *du Code pénal social*
- *de la loi du 3 août 2012 portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions*
- *de la loi du 28 février 2013 introduisant le Code de droit économique*

3.1. Généralités

36. L'article 23 du RGPD autorise les États membres à prévoir, dans certaines limites déterminées et pour des objectifs spécifiques, des exceptions aux droits des personnes concernées.
Les objectifs spécifiques pour lesquels cela est possible sont énumérés à l'article 23.1 du RGPD ; il s'agit notamment d'objectifs d'intérêt public de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale, en particulier une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique.

---

[8] Voir WP 251 "*Guidelines on Automated individual decision-making and Profiling fort he purposes of Regulation 2016/679*" du Groupe de travail Article 29, revues pour la dernière fois et adoptées le 6 février 2018 (voir https://www.privacycommission.be/sites/privacycommission/files/documents/Guidelines_automated_decision_making_profiling_0.pdf).

En tant que mesures appropriées, le Groupe de travail Article 29 mentionne notamment : des mesures spécifiques pour la minimisation des données, dont des délais de conservation maximaux, l'utilisation de techniques d'anonymisation et de pseudonymisation, un mécanisme pour une intervention humaine, l'organisation d'un audit (externe), ... (voir la p. 32 du WP 29 du Groupe de travail Article 29).

La transparence relative au traitement est bien entendu également cruciale (voir la p. 27 du WP 251 du Groupe de travail Article 29). Ce n'est que dans ces conditions que la personne concernée sera peut-être en mesure de réfuter les 'présomptions de fraude sociale' à son encontre (voir la p. 10 de l'Exposé des motifs).

Voir également l'avis n° 01/2017 de la Commission du 17 janvier 2007 *sur un avant-projet de loi relatif à certains traitements de données à caractère personnel par le Service public fédéral Finances* (p. 10-12).

[9] Cela répond aux exigences de l'article 8 de la CEDH, de l'article 22 de la Constitution et des articles 6 et 22 du RGPD.

37. Toute mesure législative prévoyant des limitations aux droits de la personne concernée doit au moins contenir des dispositions spécifiques relatives aux éléments énumérés à l'article 23.2 du RGPD, comme :
    - les finalités du traitement ou les catégories de traitement,
    - les catégories de données à caractère personnel,
    - l'étendue des limitations introduites,
    - les garanties destinées à prévenir les abus ou l'accès ou le transfert illicites,
    - la détermination du (des) responsable(s) du traitement (ou des catégories de responsables du traitement),
    - les durées de conservation,
    - les risques pour les droits et libertés des personnes concernées et
    - le droit des personnes concernées d'être informées de la limitation.

38. Afin de déterminer la portée de la marge d'évaluation dont le législateur bénéficie dans ce cadre, il importe de rappeler la jurisprudence de la Cour de justice concernant l'article 13 de la Directive 95/46/CE qui prévoyait un fondement d'exception similaire. Dans l'arrêt *Smaranda Bara*, la Cour a confirmé que ces exceptions ne pouvaient être instaurées que par "*des mesures législatives*"[10]. Ultérieurement, la Cour a précisé que les États membres ne pouvaient adopter ces exceptions que pour autant qu'elles soient "*nécessaires*"[11]. Vu l'intention inchangée du législateur européen d'assurer un niveau de protection élevé[12], cela signifie que les exceptions aux droits des personnes concernées doivent rester dans les limites du strict nécessaire[13]. La nécessité et la proportionnalité des mesures concernées doivent donc être interprétées de manière restrictive.

3.2. Limitations dans le cadre de la lutte contre le travail illégal et la fraude sociale

39. Les articles 61 à 68 de l'avant-projet de loi apportent plusieurs modifications au Code pénal social, en particulier dans le Chapitre 5 du Titre 5 concernant la '*Réglementation de certains aspects de l'échange électronique d'information entre les acteurs de la lutte contre le travail illégal et la fraude sociale*'.

---

[10] Cour de justice, 1er octobre 2015 (C-201/14), *Smaranda Bara e.a.*, § 39 ; Cour de justice, 27 septembre 2017 (C-73/16), *Puškár*, § 96.

[11] Cour de justice, 7 novembre 2013 (C-473/12), *IPI c. Englebert*, § 32.

[12] Considérant 10 du RGPD, considérant 10 de la Directive 95/46/CE.

[13] Ibid., § 39.

40. En particulier un nouveau Chapitre 5/1 intitulé "*Dispositions relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en droit pénal social*" est inséré.

L'avant-projet de loi prévoit une limitation de plusieurs droits des personnes concernées, plus précisément ceux prévus aux articles 13 et 14 du RGPD (droit à l'information), à l'article 15 du RGPD (droit d'accès), à l'article 16 du RGPD (droit de rectification) et à l'article 18 du RGPD (droit à la limitation du traitement), et ce toujours en vue de garantir "*les objectifs d'intérêt public de la sécurité sociale*".

41. En application de l'article 23.2 du RGPD, l'avant-projet de loi prévoit les dispositions spécifiques suivantes, qui sont presque identiques pour la possibilité de limitation des différents droits[14], plus précisément :
    - en ce qui concerne la <u>finalité</u> du traitement : "*en vue de garantir les objectifs d'intérêt public de la sécurité sociale*", plus précisément "*la préparation, l'organisation, la gestion et le suivi des enquêtes* (...)*en ce compris les procédures visant à l'application éventuelle d'une amende administrative ou sanction administrative* (...)" ;
    - en ce qui concerne les <u>catégories de données à caractère personnel</u> : (toutes) *les données à caractère personnel dont les services d'inspection sociale* (et les autres responsables du traitement mentionnés) sont responsables du traitement, dans la mesure où celles-ci ne sont pas *étrangères à l'objet de l'enquête ou du contrôle* ;
    - en ce qui concerne l'<u>étendue</u> des limitations :
        - pendant la période au cours de laquelle la personne concernée fait l'objet d'un contrôle ou d'une enquête (y compris les actes préparatoires de maximum 1 an après réception de la demande d'exercice du droit) et pendant la période en vue d'exercer les poursuites en la matière ;
        - dans la mesure où l'exercice des droits nuirait aux besoins du contrôle, de l'enquête ou des actes préparatoires ou risque de violer le secret de l'enquête pénale.
    - en ce qui concerne les <u>garanties visant à prévenir un abus ou un accès ou une transmission illicite</u> :
        - le DPO consigne les motifs de fait ou de droit sur lesquels se fonde sa décision et ces informations sont mises à la disposition de l'autorité de contrôle compétente ;
    - en ce qui concerne la détermination des <u>responsables du traitement</u> :

[14] D'un point de vue légistique technique, on peut se demander dans quelle mesure reprendre chaque fois intégralement les mêmes dispositions/procédures spécifiques pour la limitation de chaque droit de la personne concernée n'en complique pas la lisibilité.

- *les services d'inspection sociale visés dans le Code pénal social et dans l'arrêté royal du 1er juillet 2011*[15]*;*
- *la Direction des amendes administratives de la Division des études juridiques, de la documentation et du contentieux du SPF ETCS ;*
- *le Service des amendes administratives ou la Direction concurrence loyale de l'INASTI ;*
- *le Service d'inspection pour la contrôle des caisses d'assurances sociales pour indépendants ;*
- *le Service du contrôle administratif ou le Service d'évaluation et de contrôle médicaux de l'INAMI ;*
- *le Service d'Information et de Recherche sociale ;*

- en ce qui concerne les durées de conservation : sur ce point, l'avant-projet de loi ne prévoit rien ;
- en ce qui concerne les risques pour les droits et libertés des personnes concernées :
  - le DPO informe la personne concernée de la possibilité d'introduire une réclamation auprès de l'autorité de contrôle compétente ou de former un recours juridictionnel ;
  - le DPO consigne les motifs de fait ou de droit sur lesquels se fonde sa décision et ces informations sont mises à la disposition de l'autorité de contrôle compétente ;
  - le DPO informe sans délai la personne concernée de la levée de la limitation, immédiatement après la clôture du contrôle ou de l'enquête (à moins que le dossier ne soit transmis au Ministère public ou à l'institution compétente pour statuer sur les conclusions de l'enquête) ;
- en ce qui concerne le droit de la personne concernée d'être informée de la limitation :
  - *dans les meilleurs délais, et en tout état de cause dans un délai d'un mois à compter de la réception de la demande* (+ 2 mois en cas de demandes complexes ou répétées) ;
  - *les motifs du refus ou de la limitation ;*
  - *SAUF SI la communication risque de compromettre les objectifs d'intérêt public de la sécurité sociale.*

42. La Commission prend acte des dispositions spécifiques que l'avant-projet de loi prévoit aux articles 62 et suivants pour encadrer la possibilité de limiter certains droits des personnes concernées par les services d'inspection sociale qui y sont mentionnés, mais une disposition spécifique relative "*aux durées de conservation et aux garanties applicables, en tenant*

[15] Arrêté royal du 1er juillet 2011 *portant exécution des articles 16, 13°, 17, 20, 63, 70 et 88 du Code pénal social et fixant la date d'entrée en vigueur de la loi du 2 juin 2010 comportant des dispositions de droit pénal social*.

compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement" fait défaut. L'avant-projet de loi doit donc être complété sur ce point.

43. La Commission estime en outre que, dans la mesure où l'avant-projet de loi prévoit que le DPO du responsable du traitement informe la personne concernée des possibilités d'introduire une réclamation auprès de l'autorité de contrôle compétente ou de former un recours juridictionnel, il n'est pas tout à fait en accord avec les articles 17[16] et 42, § 4[17] de l'avant-projet de loi *relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*.

44. La Commission fait enfin remarquer que le ministère public dispose encore d'autres possibilités de règlement (comme l'avertissement contrôlé, la probation prétorienne, ...) que celles énumérées à l'article 62, avant-dernier alinéa, à l'article 64, avant-dernier alinéa, à l'article 66, avant-dernier alinéa et à l'article 68, avant-dernier alinéa de l'avant-projet de loi.

3.3. Limitations dans le cadre du contrôle, de l'inspection ou de la réglementation dans le domaine fiscal

45. Les articles 71 à 79 inclus de l'avant-projet de loi apportent plusieurs modifications dans la loi du 3 août 2012 *portant dispositions relatives aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances dans le cadre de ses missions*, en particulier l'intitulé de la section 10, chapitre 2 est remplacé comme suit : '*Le droit d'information lors de la collecte de données à caractère personnel et de communication des données à caractère personnel, le droit d'accès aux données à caractère personnel, le droit de rectification et le droit à la limitation du traitement* '.

46. Avec la section 10 susmentionnée, l'avant-projet de loi prévoit une limitation de plusieurs droits des personnes concernées, plus précisément ceux prévus aux articles 13 et 14 du RGPD (droit à l'information), à l'article 16 du RGPD (droit d'accès), à l'article 15 du RGPD (droit de rectification) et à l'article 18 du RGPD (droit à la limitation du traitement), et ce toujours afin de garantir "*les objectifs d'intérêt public dans le cadre des missions de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique dans le domaine fiscal*".

---

[16] Article 17 : "*Lorsque les données à caractère personnel figurent dans une décision judiciaire ou un dossier judiciaire, ou font l'objet d'un traitement lors d'une enquête judiciaire et d'une procédure pénale, les droits visés aux articles 12 à 22 et 34 du Règlement sont exercés conformément au Code judiciaire et au Code d'instruction criminelle.*"

[17] Article 42, § 4 : "*Les droits visés dans ce chapitre pour ce qui concernent les traitements de données des cours et tribunaux du droit commun et le ministère public sont exercés exclusivement dans les limites et dans le cadre des règles et des modalités précisées dans le Code judiciaire, le Code d'instruction criminelle et les lois particulières.*"

47. En application de l'article 23.2 du RGPD, l'avant-projet de loi prévoit également ici plusieurs dispositions spécifiques pour encadrer la possibilité de limiter certains droits des personnes concernées, qui sont presque identiques à celles prévues dans le cadre de l'inspection sociale, telles que définies au point 41, certes à la différence près que la détermination des responsables du traitement se limite, dans le texte de l'avant-projet même, au renvoi au 'SPF Finances' au complet, sans plus.

    Certes, l'Exposé des motifs (p. 40 et 41) spécifie[18] les responsables du traitement au sein du SPF Finances qui sont visés ; plus précisément :

    - les services de contrôle de l'Administration générale de la fiscalité,
    - les services de l'Administration générale de l'Inspection spéciale des impôts,
    - les services compétents de l'Administration générale de la Documentation patrimoniale,
    - les services compétents de l'Administration générale des douanes et accises.

    La Commission prend acte de la précision dans l'Exposé des motifs mais recommande néanmoins, par analogie avec l'inspection sociale (voir le point 41), de désigner dans l'avant-projet de loi même la détermination des responsables du traitement au sein du SPF Finances qui, le cas échéant, peuvent recourir à la possibilité de limiter les droits des personnes concernées.

48. La Commission prend également acte des autres dispositions spécifiques que l'avant-projet de loi prévoit aux articles 73 et suivants pour encadrer la possibilité de limiter certains droits des personnes concernées par le SPF Finances mais ici aussi, une disposition spécifique relative "*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*" fait défaut. L'avant-projet de loi doit donc être complété sur ce point.

49. La Commission estime en outre que, dans la mesure où l'avant-projet de loi prévoit que le DPO du responsable du traitement informe la personne concernée des possibilités d'introduire une réclamation auprès de l'autorité de contrôle compétente ou de former un recours juridictionnel, il n'est pas tout à fait en accord avec les articles 17 (voir la note de bas de page n° 16) et 42, § 4 (voir la note de bas de page n° 17) de l'avant-projet de loi *relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*..

[18] L'Exposé des motifs renvoie en la matière à l'arrêté royal *organique des services opérationnels du Service public fédéral Finances* du 3 décembre 2009.

50. La Commission fait enfin remarquer que le ministère public dispose encore d'autres possibilités de règlement (comme l'avertissement contrôlé, la probation prétorienne, ...) que celles énumérées à l'article 73, avant-dernier alinéa, à l'article 75, avant-dernier alinéa, à l'article 77, avant-dernier alinéa et à l'article 79, avant-dernier alinéa de l'avant-projet de loi.

3.4. Limitations dans le cadre de l'inspection et du contrôle par les services dont les compétences sont définies dans le Code de droit économique

51. Les articles 82 et 83 de l'avant-projet de loi apportent plusieurs modifications dans la loi du 28 février 2013 *introduisant le Code de droit économique*. Dans le Titre 1er, Chapitre 1er du livre XV ("*L'exercice de la surveillance et la recherche et la constatation des infractions*"), il est inséré 2 nouveaux articles relatifs à la manière dont il est donné suite à la demande de celui dont les données à caractère personnel sont traitées par les services d'inspection et de contrôle du SPF Économie en vue d'exercer ses droits prévus aux articles 12 à 22 du RGPD, et ce en application de l'article 23 du RGPD.

52. L'avant-projet de loi prévoit à l'article 82 une limitation de tous les droits des personnes concernées, plus précisément de ceux prévus aux articles 12 à 22 et 34 du RGPD, et ce toujours afin de garantir "*l'article 23.1, d, g et h*" et ce dans le chef des "*services d'inspection et/ou de contrôle dont les compétences sont définies par le Code de droit économique*".

53. La Commission constate tout d'abord que la formulation de l'article 82 (en particulier les premier et troisième alinéas) de l'avant-projet de loi laisse à désirer en termes de clarté ; en outre, le texte en néerlandais ne correspond pas au texte en français.

54. L'article 82 de l'avant-projet de loi prévoit une exception générale formulée de manière extrêmement large à tous les droits prévus - aux articles 12 à 22 et 34 du RGPD - des personnes concernées dans le chef de tous les services de contrôle et d'inspection au sein du SPF Économie (pas de disposition précise qui identifie concrètement les responsables du traitement) avec un simple renvoi à l'article 23.1, d, g et h du RGPD sans la moindre précision des missions réglementaires des services de contrôle et d'inspection qui sont visés. Le RGPD n'autorise pas un tel 'chèque en blanc'.

55. L'article 83 de l'avant-projet de loi ne tient nullement compte non plus des dispositions spécifiques minimales requises par l'article 23.2 du RGPD et offre à peine une plus-value pour garantir le maintien de l'essence des libertés et droits fondamentaux dans une société démocratique (sauf éventuellement l'indication de la durée de conservation - toutefois très large - qui ne peut pas dépasser les délais de prescription des infractions recherchées/visées).

En effet, la Commission n'est pas en faveur d'un système d'accès indirect avec intervention de l'APD où la personne concernée ne reçoit qu'un message précisant que "*les vérifications nécessaires ont été effectuées*" Il s'agit effectivement d'un système lourd et administrativement pesant qui exclut une réelle possibilité de recours en la matière auprès de l'APD. En outre, on ne justifie aucunement les raisons pour lesquelles un tel système d'accès indirect (qui n'est appliqué presque nulle part en Europe) serait indispensable pour les services d'inspection économique[19], alors que les services d'inspection sociale et financière peuvent de toute évidence parfaitement fonctionner sans un tel système.

56. La Commission doit en conclure que les articles 82 et 83 ne réussissent pas le test de l'article 23 du RGPD. La Commission se permet de faire référence à la manière dont l'article 23 du RGPD est appliqué dans l'avant-projet de loi pour les services d'inspection sociale (voir les articles 62 à 68 de l'avant-projet de loi) et les services de contrôle et d'inspection du SPF Finances (voir les articles 73 à 79 inclus de l'avant-projet de loi) et suggère une application similaire pour les services de contrôle et d'inspection économique (qui doivent quoi qu'il en soit encore être définis).

4. DIVERS

57. Outre ce qui précède, plusieurs autres objections et remarques peuvent encore être formulées concernant diverses dispositions tout au long du texte de l'avant-projet de loi.

58. La Commission recommande dans un premier temps de remplacer à l'article 5, dernier alinéa de l'avant-projet de loi le 'secret professionnel' par une 'obligation de confidentialité'.

59. En vertu de l'article 11 de l'avant-projet de loi, la finalité du datawarehouse existant de la BCSS est considérablement étendue. Auparavant, il servait à "*la réalisation de recherches pouvant être utiles à la connaissance, à la conception et à la gestion de la sécurité sociale*". En vertu de l'article 11 de l'avant-projet de loi, il pourra servir n'importe quelle fin historique, statistique, scientifique ou de soutien à la politique.

[19] Dans tous les cas, une reformulation de l'article 82, *in fine*, et de l'article 83, 3°, *in fine*, qui ne couvrent pas nécessairement la même portée s'impose. Ensuite, il n'est pas clair de savoir comment l'intervention de l'APD en tant qu'intermédiaire doit prévenir 'les abus ou l'accès ou le transfert illicite'.

60. La Commission estime que les remarques formulées aux points 26 et suivants concernant la base légale créée dans l'article 12 de l'avant-projet de loi en vue de la création d'un ou de plusieurs datawarehouse(s) par les institutions de sécurité sociale et les services d'inspection sociale à des fins de datamatching et de datamining dans le cadre d'une lutte efficace contre la fraude sociale peuvent également être rappelées ici.

61. La base juridique étendue en vertu de l'article 11 de l'avant-projet de loi pour le datawarehouse de la BCSS ne tient pas compte des exigences de l'article 8 de la CEDH et de l'article 22 de la Constitution, ni de celles des articles 6.3 et 22 du RGPD.

62. La Commission estime en outre que l'article 13 de l'avant-projet de loi souffre aussi du même mal. Dans la mesure où il est prévu que les institutions de sécurité sociale, les services d'inspection sociale et la Direction des amendes administratives de la division des études juridiques, de la documentation et du contentieux du SPF ETCS puissent également traiter ultérieurement, dans le cadre d'une autre mission légale (sans plus de précision), chaque donnée à caractère personnel qu'ils traitent dans le cadre de l'exécution de leurs missions légales , l'article 13 de l'avant-projet de loi viole les articles 6.3 et 6.4 du RGPD.

63. En effet, lorsque le traitement pour une autre finalité que celle pour laquelle les données à caractère personnel ont été collectées n'est pas fondé pas sur le consentement de la personne concernée ou sur le droit d'un État membre[20], la compatibilité de la finalité envisagée avec la finalité pour laquelle les données ont été collectées doit être évaluée par le responsable du traitement en tenant compte :
    - du lien entre les deux finalités ;
    - de la relation entre les personnes concernées et le responsable du traitement ;
    - de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données à caractère personnel (art. 9 et 10 du RGPD) ;
    - des conséquences possibles du traitement prévu pour les personnes concernées ;
    - de l'existence de garanties appropriées, qui peuvent comprendre le cryptage ou la pseudonymisation.

[20] Qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23.1 du RGPD et qui tient compte des exigences de l'article 8 de la CEDH, de l'article 22 de la Constitution et des articles 6.3 et 22 du RGPD, ce qui n'est pas du tout valable pour l'article 13 de l'avant-projet de loi.

64. L'article 11 de l'avant-projet de loi attribue à la BCSS le rôle d' 'organisation intermédiaire' et l'article 46 de l'avant-projet de loi fait de même pour la plate-forme eHealth. Il n'y a toutefois nulle part dans l'avant-projet de loi une définition d' 'organisation intermédiaire', d'autant plus que le renvoi à la définition "*en vertu 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*" disparaît.

65. La Commission estime que le droit à la limitation du traitement, tel que prévu à l'article 18 du RGPD, n'entrave nullement une bonne exécution par les institutions de sécurité sociale de leurs missions légales et réglementaires dans le cadre de notre système de sécurité sociale. Les institutions de sécurité sociale ont, au contraire, tout intérêt à disposer à tout moment de données à caractère personnel correctes de toutes les personnes concernées. La Commission recommande dès lors de supprimer l'article 14 de l'avant-projet de loi.

66. L'article 20, point b de l'avant-projet de loi donnera peut-être lieu à une circulation de données incorrectes, dans la mesure où il prévoit que des corrections et des effacements de données sociales à caractère personnel ne seront communiqués qu'à la personne concernée elle-même. La Commission renvoie en la matière à sa recommandation d'initiative n° 09/2012 *relative aux sources authentiques de données dans le secteur public* (en particulier aux points 17 et suivants).

67. La Commission fait enfin remarquer que dans la mesure où dans l'adaptation de diverses réglementations, l'avant-projet de loi se limite au simple remplacement de la dénomination '(la section sécurité sociale/la section santé du) Comité sectoriel de la Sécurité sociale et de la Santé' par 'la chambre sécurité sociale et santé du comité de sécurité de l'information', il n'affecte pas la compétence d'autorisation pour certains flux de données, ce qui engendre une incohérence avec la (re)formulation des compétences du CIS de rendre des délibérations (voir notamment les articles 40, 46, 51, 58, 59 et 85 de l'avant-projet de loi).

III. CONCLUSION

68. Étant donné que la Commission est acquise à une initiative où les DPO et les responsables du traitement sont soutenus par des délibérations consultatives, elle est favorable à la création du CSI.

    Néanmoins, la Commission estime - vu ce qui précède - que l'avant-projet de loi n'est pas tout à fait conforme aux dispositions du RGPD, en particulier vu :

- la qualification des délibérations que doit rendre le CSI de "*décisions de portée générale contraignante*", dans la mesure où l'APD serait également liée par ces décisions (voir le point 11) ;
- que l'accent n'est pas suffisamment mis sur l'indépendance du DPO (voir les points 15 à 18 inclus) ;
- l'absence de disposition prévoyant un avis préalable de l'APD en cas d'intervention éventuelle du Roi pour fixer les règles selon lesquelles le DPO d'une institution de sécurité sociale doit exercer des missions complémentaires (voir le point 19) ;
- le besoin de retravailler la composition du CSI (voir les points 21 à 25 inclus) ;
- le 'chèque en blanc' délivré par l'article 12 de l'avant-projet de loi pour la création d'un (de) datawarehouse(s) à des fins de datamatching et de datamining en vue d'une lutte efficace contre la fraude sociale, contraire à l'article 8 de la CEDH, à l'article 22 de la Constitution et aux articles 6.3 et 22 du RGPD (voir les points 29 et suivants) ;
- la lacune et les imperfections dans les dispositions spécifiques que l'avant-projet de loi prévoit pour encadrer la possibilité de limiter certains droits des personnes concernées dans le chef des services d'inspection sociale et financière/fiscale, conformément à l'article 23 du RGPD (voir les points 42 à 44 et 48 à 50) ;
- l'incompatibilité des articles 83 et 83 de l'avant-projet de loi concernant la limitation des droits des personnes concernées dans le chef des services d'inspection économique avec l'article 23 du RGPD (voir le point 56) ;
- la mention à l'article 5, dernier alinéa, de l'avant-projet de loi du 'secret professionnel' plutôt que d'une 'obligation de confidentialité' (voir le point 58) ;
- le 'chèque en blanc' délivré par l'article 11 de l'avant-projet de loi pour la base juridique étendue pour le datawarehouse de la BCSS, contraire à l'article 8 de la CEDH, à l'article 22 de la Constitution et aux articles 6.3 et 22 du RGPD (voir le point 61) ;
- l'incompatibilité de l'article 13 de l'avant-projet de loi avec les articles 6.3 et 6.4 du RGPD (voir le point 62) ;
- l'absence d'une définition d' 'organisation intermédiaire' (voir le point 64) ;
- la dérogation superflue à l'article 18 du RGPD par l'article 14 de l'avant-projet de loi (voir le point 65) ;
- l'incompatibilité de l'article 20, point b, de l'avant-projet de loi avec la recommandation n° 09/2012 (voir le point 66) ;
- le maintien de la compétence d'autorisation pour certains flux de données, ce qui engendre une incohérence avec la (re)formulation des compétences du CSI de rendre des délibérations (voir le point 67).

PAR CES MOTIFS,

concernant l'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*, la Commission émet

- un avis favorable quant au principe de l'instauration d'un CSI ;
- un avis défavorable concernant les points évoqués dans la conclusion au point 68.

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere