Numéro du rôle : 6552
Arrêt n° 29/2018 du 15 mars 2018

A R R E T

En cause : le recours en annulation partielle de la loi du 13 mai 2016 « modifiant la loi-programme (I) du 29 mars 2012 concernant le contrôle de l'abus d'adresses fictives par les bénéficiaires de prestations sociales, en vue d'introduire la transmission systématique de certaines données de consommation de sociétés de distribution et de gestionnaire de réseaux de distribution vers la BCSS améliorant le datamining et le datamatching dans la lutte contre la fraude sociale », introduit par l'ASBL « Ligue des Droits de l'Homme ».

La Cour constitutionnelle,

composée des présidents A. Alen et J. Spreutels, des juges L. Lavrysen, J.-P. Moerman, E. Derycke et F. Daoût, et, conformément à l'article 60*bis* de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, du président émérite E. De Groot, assistée du greffier P.-Y. Dutilleux, présidée par le président émérite E. De Groot,

*

* *

I. *Objet du recours et procédure*

Par requête adressée à la Cour par lettre recommandée à la poste le 28 novembre 2016 et parvenue au greffe le 29 novembre 2016, l'ASBL « Ligue des Droits de l'Homme », assistée et représentée par Me R. Jespers, avocat au barreau d'Anvers, a introduit un recours en annulation partielle de la loi du 13 mai 2016 « modifiant la loi-programme (I) du 29 mars 2012 concernant le contrôle de l'abus d'adresses fictives par les bénéficiaires de prestations sociales, en vue d'introduire la transmission systématique de certaines données de consommation de sociétés de distribution et de gestionnaire de réseaux de distribution vers la BCSS améliorant le datamining et le datamatching dans la lutte contre la fraude sociale » (publiée au *Moniteur belge* du 27 mai 2016).

Le Conseil des ministres, assisté et représenté par Me V. Pertry, avocat au barreau de Bruxelles, a introduit un mémoire, la partie requérante a introduit un mémoire en réponse et le Conseil des ministres a également introduit un mémoire en réplique.

Par ordonnance du 26 septembre 2017, la Cour, après avoir entendu les juges-rapporteurs A. Alen et J.-P. Moerman, a décidé que l'affaire était en état, qu'aucune audience ne serait tenue, à moins qu'une partie n'ait demandé, dans le délai de sept jours suivant la réception de la notification de cette ordonnance, à être entendue, et qu'en l'absence d'une telle demande, les débats seraient clos le 18 octobre 2017 et l'affaire mise en délibéré.

Aucune demande d'audience n'ayant été introduite, l'affaire a été mise en délibéré le 18 octobre 2017.

Les dispositions de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle relatives à la procédure et à l'emploi des langues ont été appliquées.

II. *En droit*

- *A* -

A.1. La partie requérante prend un moyen unique, formulé en plusieurs griefs, (1) de la violation des articles 10, 11 et 22 de la Constitution, combinés ou non avec les articles 8, 14, 17 et 18 de la Convention européenne des droits de l'homme, avec les articles 7, 8 et 52 de la Charte des droits fondamentaux de l'Union européenne, avec l'article 17 du Pacte international relatif aux droits civils et politiques, et avec les principes généraux du droit de la sécurité juridique et de la proportionnalité; et (2) de la violation des articles 6, 7, 10, 11, 14, 16 et 17 de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données » (ci-après : la directive 95/46/CE); des articles 5, 6, 7, 12, 13, 17, 18, 21, 28 et 29 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 « relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) »; et des articles 4, 5, 9, 10 et 16 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 (ci-après : la loi sur la protection de la vie privée).

Quant à la recevabilité

A.2. Le Conseil des ministres soulève l'irrecevabilité partielle du recours en raison, d'une part, de l'incompétence de la Cour et, d'autre part, de l'absence d'un exposé des griefs.

A.3.1. Le Conseil des ministres estime que le moyen unique est irrecevable en ce qu'il allègue directement la violation des articles 6, 7, 10, 11, 14, 16 et 17 de la directive 95/46/CE, et des articles 5, 6, 7, 12, 13, 17 et 18 du règlement général sur la protection des données, étant donné que la Cour n'est pas compétente pour contrôler directement les dispositions attaquées au regard du droit dérivé de l'Union.

A.3.2. Il relève également qu'il n'appartient pas à la Cour de se prononcer sur la violation alléguée des articles 4, 5, 9 et 10 de la loi sur la protection de la vie privée en ce que ces articles ne mettent pas en œuvre les obligations internationales prescrites par le règlement général sur la protection des données et par la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

A.3.3. Il observe enfin que la Cour n'est pas non plus compétente pour apprécier la compatibilité de (futures) mesures d'exécution avec les normes de référence invoquées.

A.4. Le Conseil des ministres estime que l'on n'aperçoit pas toujours clairement sous quel angle les dispositions attaquées violeraient les normes de référence invoquées. Il affirme tout d'abord que la partie requérante n'expose nullement pourquoi les articles 17 et 18 de la Convention européenne des droits de l'homme seraient violés ni pourquoi les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne trouveraient à s'appliquer. En ce qui concerne ce dernier élément, il affirme que la partie requérante néglige de démontrer que les dispositions attaquées mettraient en œuvre le droit de l'Union. Il souligne que cela vaut également pour les articles 17 et 18, invoqués, du règlement général sur la protection des données.

A.5. La partie requérante conteste l'exception d'irrecevabilité du recours.

A.6.1. Elle affirme que la Cour est compétente pour opérer un contrôle indirect au regard du règlement général sur la protection des données et de la directive 95/46/CE parce que ces dispositions forment un ensemble avec les garanties prescrites par l'article 22 de la Constitution, lues en combinaison avec des droits fondamentaux comparables énoncés dans des dispositions conventionnelles. Elle souligne en outre que les articles de la loi sur la protection de la vie privée sont la transposition de la directive précitée.

A.6.2. Elle considère également que la critique portant sur l'exposé défectueux des griefs n'est pas fondée et qu'elle a suffisamment expliqué en quoi les normes de référence sont violées.

Quant au moyen unique

A.7. La partie requérante invoque en ordre principal la violation de l'article 22 de la Constitution, combiné ou non avec l'article 8 de la Convention européenne des droits de l'homme, avec l'article 17 du Pacte international relatif aux droits civils et politiques, avec l'article 6.1, b) et c), de la directive 95/46/CE, avec l'article 5.1, b) et c), du règlement général sur la protection des données, et avec l'article 4, § 1er, 2° et 3°, de la loi sur la protection de la vie privée, parce que la mesure attaquée ne répond pas aux exigences en matière de légalité, de nécessité, de subsidiarité et de proportionnalité.

A.8. Elle affirme que le traitement de données de consommation relative à l'eau, au gaz et à l'électricité par le système dit « push », introduit par la loi attaquée, méconnaît le principe de limitation des finalités prescrit par l'article 6.1, b), de la directive 95/46/CE, par l'article 5.1, b), du règlement général sur la protection des données, et par l'article 4, § 1er, 2°, de la loi sur la protection de la vie privée. Elle affirme que ce traitement sert une autre finalité que la facturation. Elle souligne que les données de consommation dont disposent les sociétés de distribution et les gestionnaires de réseaux de distribution ont été obtenues en vue de la facturation de cette consommation et du suivi statistique des évolutions de consommation, et non dans le but de lutter contre la fraude sociale.

A.9. La partie requérante fait valoir que le système « push », introduit par la loi attaquée, impose aux sociétés de distribution et aux gestionnaires de réseaux de distribution une obligation de conservation générale et

de longue durée afin que les services publics sociaux puissent procéder au « data mining ». Elle estime qu'il s'agit d'un stockage général de données sans distinction qui, et sans tenir compte de l'accès proprement dit aux données, constitue selon elle une violation des dispositions précitées. Elle se réfère à cet égard à la jurisprudence en matière de données de télécommunications (voy. notamment CJUE, grande chambre, 8 avril 2014, C-293/12, *Digital Rights Ireland Ltd*, et C-594/12, *Kärntner Landesregierung e.a.*). Elle affirme que le mécanisme attaqué concerne des données qui permettent de tirer des conclusions très précises par rapport à la vie privée d'un nombre important de personnes. Elle relève en effet qu'il s'agit d'une forme de « data mining » qui touche tous les consommateurs privés de gaz, d'électricité et d'eau parce qu'elle est effectuée sur la base des données de consommation et de la composition du ménage. Elle souligne que le système « push » aboutit au traitement de données de citoyens qui ne bénéficient pas d'allocations. Elle épingle le fait qu'il s'agit d'un traitement non différencié et à grande échelle de données à caractère personnel, sans garanties spécifiques suffisantes, même si au fil des différentes phases, le nombre de personnes concernées diminue. Le système attaqué a donc des effets disproportionnés pour un groupe important de personnes, sans qu'il y ait des indices de fraude au domicile.

A.10. Elle affirme que le système de « data mining » imposé, qui a pour but d'identifier, parmi une très grande quantité de données relatives à la consommation en eau, gaz et électricité, après examen par l'inspection sociale ou par l'institution publique de sécurité sociale (ci-après : IPSS), les allocataires sociaux qui perçoivent une prestation trop élevée grâce à une fraude au domicile, n'est pas raisonnablement proportionné par rapport au droit au respect de la vie privée.

Elle fait valoir que le législateur a négligé d'imposer des garanties spécifiques relatives à la protection de la vie privée des personnes concernées (1) aux sociétés de distribution et aux gestionnaires de réseaux de distribution, (2) à la Banque-carrefour de la sécurité sociale (ci-après : la BCSS) et (3) aux IPSS et aux inspecteurs sociaux. Elle se réfère à la jurisprudence concernant les services de communications électroniques.

A.11. Selon la partie requérante, le législateur ne démontre pas la nécessité de développer un système aussi excessif dans le cadre de la lutte contre la fraude sociale. Elle relève qu'avant d'adopter la loi attaquée, le législateur avait introduit, par la loi-programme du 29 mars 2012, un système dit « pull » qui permettait aux inspecteurs sociaux d'exiger la production des données de consommation.

Elle souligne que dans le système « pull », en cas de présomption d'utilisation d'une adresse fictive, les inspecteurs sociaux pouvaient déjà exiger cette production, ce qui n'impliquait qu'une ingérence limitée dans le droit au respect de la vie privée des allocataires sociaux. Elle relève que le système « pull » n'a jamais été mis en œuvre plus concrètement et que le législateur n'a pas non plus présenté de statistiques relatives à l'examen de la consommation par l'inspection sociale, de sorte que, selon elle, il n'y a aucun élément attestant de la non-efficacité éventuelle du système « pull » pour lutter contre la fraude sociale au domicile. Elle constate que dans le cadre du système « push », un projet-pilote sera mis en place, ce qui signifie, selon elle, qu'il est question d'une mesure qui ne repose pas sur une base rationnelle et scientifique.

Elle estime par conséquent que la nécessité d'évoluer vers le système « push » actuellement introduit n'a pas été démontrée.

A.12. Elle ajoute que le législateur a négligé de vérifier, compte tenu de l'impact sur la vie privée, le caractère suffisant des moyens ou des méthodes existants pour lutter contre la fraude sociale au domicile. Elle souligne en effet que les services publics sociaux disposent déjà de plusieurs moyens pour détecter la fraude, tels que les visites domiciliaires, l'audition des personnes concernées et de témoins, ou la possibilité d'exiger la production des données de consommation, ce qui signifie que le système « push » va au-delà de ce qui est strictement nécessaire.

A.13. En ordre subsidiaire, la partie requérante critique l'absence de plusieurs garanties dans le cadre du mécanisme attaqué, ou leur caractère insuffisant.

A.14. Elle allègue la violation du principe de transparence, tel qu'il résulte de l'article 22 de la Constitution, de l'article 8 de la Convention européenne des droits de l'homme, de l'article 17 du Pacte international relatif aux droits civils et politiques, des articles 6.1, a) et c), et 10, de la directive 95/46/CE, des articles 5.1, a), 12 et 21 du règlement général sur la protection des données, et de l'article 4, § 1er, 1° et 3°, de la loi sur la protection de la vie privée.

A.15. Elle estime que la référence à la loi sur la protection de la vie privée a pour effet de ne pas exclure l'application de l'article 3, § 5, 3°, de cette loi dans le cadre du système attaqué. Elle souligne que l'arrêté royal

du 11 mars 2015 « portant exécution de l'article 3, § 5, 3°, 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 » est dès lors applicable dans le cadre du système « push », ce qui implique que les droits des personnes concernées visés aux articles 9, 10, § 1er, et 12 de la loi sur la protection de la vie privée ne peuvent être exercés que de manière indirecte par l'intervention de la Commission de la protection de la vie privée (article 13 de la loi sur la protection de la vie privée).

A.16. Elle compare en outre les garanties prévues par la loi attaquée avec celles introduites dans le cadre du traitement de données à caractère personnel par des services publics fiscaux, comparaison d'où elle déduit une inégalité de traitement. Elle souligne de surcroît que, d'une part, le mécanisme attaqué ne permet pas de s'opposer à la sélection effectuée par la technique du « data mining », et que, d'autre part, il ne prévoit pas la rédaction d'un rapport sur les devoirs d'investigation accomplis par l'inspection sociale pour confirmer ou infirmer un signal d'alerte à la fraude.

A.17. La partie requérante invoque ensuite la violation de l'article 22 de la Constitution, de l'article 6.1, e), de la directive 95/46/CE, de l'article 5.1, e), du règlement général sur la protection des données, et de l'article 4, § 1er, 5°, de la loi sur la protection de la vie privée, en ce qu'il n'est prévu aucun délai de conservation spécifique.

A.18. Elle relève que le système « push » comprend trois phases faisant intervenir différents acteurs, de sorte qu'il devrait y avoir trois délais de conservation différents. De plus, elle juge insuffisante la fixation d'un délai de conservation par le comité sectoriel pour les IPSS et pour l'inspection sociale. Elle estime en effet qu'un élément essentiel tel qu'un délai de conservation doit être fixé par le législateur lui-même, et que la délégation au comité sectoriel viole le principe de légalité.

A.19. Elle invoque encore la violation de l'article 22 de la Constitution, de l'article 8 de la Convention européenne des droits de l'homme, de l'article 17 du Pacte international relatif aux droits civils et politiques, de l'article 6.2 de la directive 95/46/CE, des articles 5.2, 28 et 29 du règlement général sur la protection des données, et de l'article 4, § 2, de la loi sur la protection de la vie privée; elle reproche au législateur de ne pas avoir prévu de responsable du traitement de l'analyse de données relationnelles.

A.20. Elle constate qu'au paragraphe 3 de l'article 101/1, tel qu'inséré par l'article 3, attaqué, le législateur a fait référence à tort à l'article 101, § 1er, de sorte qu'il n'a pas désigné le responsable du traitement des données visé audit article 101/1.

A.21. Elle fait encore valoir que pour la transmission des données aux inspecteurs sociaux, le législateur n'a pas exigé l'autorisation d'un comité sectoriel institué par la Commission de la protection de la vie privée.

A.22. Elle allègue enfin la violation des principes d'intégrité et de confidentialité tels qu'ils découlent de l'article 22 de la Constitution, de l'article 8 de la Convention européenne des droits de l'homme, de l'article 17 du Pacte international relatif aux droits civils et politiques, des articles 6.1, a) et c), et 10 de la directive 95/46/CE, de l'article 5.1, f), du règlement général sur la protection des données, et de l'article 16, § 4, de la loi sur la protection de la vie privée, en ce que le législateur n'a pas prévu de mesures de sécurité spécifiques en suffisance.

A.23. Elle estime que dans la première phase, les dispositions attaquées n'offrent pas de garanties suffisantes en matière d'intégrité et de confidentialité. Pour elle, ni la BCSS ni les IPSS ne peuvent être tenues pour responsables du traitement effectué durant la première phase. Elle considère que la loi attaquée ne prévoit pas de garanties spécifiques suffisantes en matière de sécurité durant la seconde phase de traitement par la BCSS. Elle souligne que la loi attaquée n'a pas non plus prévu, pour la troisième phase de traitement par les IPSS, de mesures de sécurité spécifiques en matière d'accès, de codage et de mise à jour périodique des données.

Elle affirme que l'article 16, § 4, de la loi sur la protection de la vie privée ne peut pas servir simplement de filet de sécurité pour les exigences en matière de sécurité. Elle souligne que le système « push » concerne un traitement massif de données à caractère personnel, alors que la loi sur la protection de la vie privée concerne des cas individuels de traitement de données. Il est donc nécessaire d'imposer des exigences plus spécifiques et plus strictes. Elle pointe également l'absence d'un organe de contrôle spécifique.

A.24. Le Conseil des ministres reconnaît que les dispositions attaquées constituent une ingérence dans le 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, mais il estime que cette ingérence peut se justifier parce qu'elle

respecte les trois exigences prévues par la jurisprudence : (1) elle a été définie par la loi, (2) elle poursuit un but légitime et (3) elle est nécessaire dans une société démocratique.

A.25. En ce qui concerne la première exigence, le Conseil des ministres relève que les dispositions attaquées ont été adoptées par une assemblée délibérante démocratiquement élue, de sorte que l'exigence de légalité formelle prescrite par l'article 22 de la Constitution a été respectée.

Il affirme également que le principe de limitation des finalités n'a pas été violé étant donné que le système « push », y compris le « data matching » et le « data mining », a été institué par la loi. Il ajoute que l'article 4, § 1er, 2°, de la loi sur la protection de la vie privée prévoit que des traitements ultérieurs sont admissibles, en l'occurrence lorsqu'ils ont été prévus par la loi, de sorte qu'aucune autorisation n'est requise.

Il estime que la mesure attaquée est suffisamment claire et précise.

A.26. En ce qui concerne la deuxième exigence, il est d'avis que les dispositions attaquées poursuivent un but légitime. Ce but consiste en effet à renforcer et à optimiser la lutte contre la fraude aux allocations sociales par fraude au domicile. Selon le Conseil des ministres, la fraude sociale met en péril le fonctionnement du tissu social parce que le système social est financé avec les deniers de la collectivité.

A.27. En ce qui concerne la troisième exigence, il insiste sur le pouvoir d'appréciation du législateur. Il est d'avis que le système « push » est nécessaire et proportionné. Il estime que les dispositions contestées répondent à un besoin social impérieux. Il relève que l'importance de la fraude sociale, plus particulièrement de la fraude au domicile, est attestée par les statistiques, entre autres, de l'Institut national d'assurance maladie-invalidité.

A.28.1. Le Conseil des ministres conteste qu'une comparaison entre plusieurs alternatives sur le plan de leur impact sur la vie privée soit un élément du contrôle de proportionnalité.

A.28.2. En ordre subsidiaire, il estime qu'aucune mesure moins radicale ne peut aboutir à un résultat comparable.

Selon lui, le système « push » permet d'agir de manière plus proactive ou plus efficace, en actionnant des clignotants, y compris dans les cas où il n'y a pas encore de présomption de fraude, alors que le système « pull » part d'une demande effectuée par un inspecteur social dans le cadre d'un dossier concret sur la base d'une présomption. Le système attaqué permet la détection de nouveaux dossiers sans qu'une fraude soit déjà présumée, ce qui augmente la possibilité de se faire prendre. Le système « push » a aussi pour effet de permettre aux inspecteurs sociaux d'examiner plus de dossiers grâce au gain de temps réalisé.

A.28.3. Il estime que le système « push » offre davantage de garanties parce que contrairement au système « pull », il n'alerte pas les sociétés de distribution et les gestionnaires de réseaux de distribution sur la situation du consommateur.

A.29. Le Conseil des ministres considère par ailleurs que le système « push » constitue un moyen approprié et nécessaire pour détecter et pour combattre la fraude au domicile. Il relève que la consommation d'énergie fournit un indice majeur sur la réalité de la résidence à une adresse donnée. Il ajoute qu'une consommation qui diffère fortement de celle qui correspond à la composition officielle du ménage peut actionner un clignotant révélant une fraude au domicile. Il affirme que le système « push » renforce la détection de la fraude, et rend cette détection plus efficace. Le système « push » vient compléter les pouvoirs actuels de l'inspection sociale, permettant à celle-ci de gagner beaucoup de temps et de travailler de manière plus ciblée. Il attire l'attention sur le fait que le nombre d'enquêtes peut ainsi augmenter, ce qui contribue à décourager la fraude au domicile.

Il souligne dès lors que la preuve a été faite de la nécessité de passer du système « pull » au système « push ». Il se réfère également aux travaux préparatoires. Il relève encore que la partie requérante se contente d'énoncer des suppositions générales et non fondées sur le caractère moins intrusif du système « pull ». Il affirme également que le législateur n'a jamais eu l'intention de tester des options stratégiques sans avoir au préalable soupesé minutieusement les avantages et les inconvénients, ce qui a vraiment été fait.

A.30.1. Selon le Conseil des ministres, les dispositions attaquées n'entraînent pas, au vu des garanties offertes, une limitation disproportionnée du droit au respect de la vie privée.

A.30.2. Il renvoie tout d'abord à l'application de la loi sur la protection de la vie privée dans le cadre des traitements contestés. Il relève encore que la structure du système « push » est telle qu'elle permet de réduire le nombre de données à caractère personnel traitées au fur et à mesure de la mise en œuvre des différentes phases (p. ex. le seuil de 80 % d'écart minimum).

A.30.3. Il souligne que l'application de l'article 4, § 1er, 5°, de la loi sur la protection de la vie privée est intégralement maintenue durant toutes les phases du système « push », de sorte qu'il y a suffisamment de garanties par rapport à la conservation des données traitées. Ainsi, les données à caractère personnel ne peuvent être conservées pendant un délai supérieur à ce qui est nécessaire pour réaliser le but poursuivi. Il précise toutefois qu'il n'y a aucune obligation d'imposer des délais de conservation légaux précis et relève que la Commission de la protection de la vie privée a recommandé de fixer les délais dans les autorisations. Il souligne encore que la délégation au comité sectoriel répond aux exigences de l'article 22 de la Constitution parce que le législateur a bel et bien fixé tous les éléments essentiels du système « push ».

Il estime dès lors qu'il y a bien trois délais de conservation différents, adaptés au contexte spécifique. Par rapport à la transmission de données par des sociétés de distribution et des gestionnaires de réseaux de distribution, il souligne que ces données ne peuvent être conservées sous une forme permettant une identification si elles ne sont plus utiles pour la réalisation de l'objet pour lequel elles ont été collectées. Quant au traitement effectué par la BCSS, cette institution ne conserve aucune donnée. Quant au traitement de données effectué par les IPSS et leurs inspecteurs sociaux, les travaux préparatoires soulignent que le délai de conservation correspond au délai de prescription de cinq ans.

A.31. Par ailleurs, il y a encore d'autres garanties qui encadrent le mécanisme attaqué.

A.32. En ce qui concerne la première phase, le traitement s'opère sous la responsabilité des sociétés de distribution et des gestionnaires de réseaux de distribution.

A.33. Il insiste ensuite sur les garanties concernant la seconde phase durant laquelle la BCSS croise les données de consommation et les transmet aux IPSS. Ce traitement s'effectue sous la responsabilité de la BCSS, dont l'intervention est requise à des fins de filtrage, de sorte qu'il n'y a pas d'échange direct de données entre, d'une part, les IPSS et, d'autre part, les sociétés de distribution et les gestionnaires de réseaux de distribution. Il renvoie à cet égard au cadre légal relatif à la BCSS, qui énonce des garanties notamment par rapport au secret professionnel et à la désignation d'un conseiller en sécurité (articles 22, 23, 24, 25 et 28 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale; ci-après : la loi BCSS). Il pointe les sanctions prévues par les articles 213 et suivants du Code pénal social lorsque la confidentialité des données n'est pas respectée ou lorsque les mesures de sécurité requises ne sont pas prises. Enfin, il fait encore remarquer que la BCSS ne peut transmettre les données à une IPSS qu'à la condition que l'institution en question octroie ou ait octroyé une allocation sociale à la personne concernée pendant la période de référence.

En ce qui concerne les mesures de sécurité, il renvoie à la loi BCSS.

A.34. Le Conseil des ministres relève également les garanties concernant la troisième phase durant laquelle les IPSS traitent les données obtenues par l'intermédiaire de la BCSS. Il renvoie à cet égard à l'article 103 de la loi-programme (I) du 29 mars 2012, qui stipule que les inspecteurs sociaux informent le bénéficiaire de la possibilité d'utiliser les données de consommation, et à l'article 79 du Code pénal social, qui règle l'accès au dossier administratif.

Il relève également que les IPSS ne peuvent utiliser les données qu'en vue de procéder à des contrôles en matière de fraude au domicile et que les données ne peuvent être traitées que pendant le délai nécessaire à la réalisation du but poursuivi. Il souligne que le comité sectoriel de la sécurité sociale et de la santé doit autoriser les IPSS à contrôler effectivement, sur la base des données transmises par la BCSS, associées à d'autres données sociales, si la prestation sociale est octroyée sur la base d'une adresse fictive. Il souligne en outre qu'il ressort de la lecture conjointe des articles 2 et 3, attaqués, que l'autorisation concerne aussi bien les IPSS que les inspecteurs sociaux. Il observe de surcroît que les inspecteurs sociaux n'ont pas besoin d'une autorisation distincte, car ils relèvent de l'autorisation donnée aux IPSS auxquelles ils sont rattachés.

Cette autorisation fixe également le délai de conservation des données codées et décodées. Il souligne l'accès limité octroyé aux inspecteurs sociaux, et le devoir de discrétion auquel ils sont soumis.

Enfin, les analyses prévues par l'article 3 attaqué, effectuées par les IPSS, sont avant tout réalisées sur la base des données codées. Ce n'est que lorsqu'un risque d'utilisation d'une adresse fictive est avéré que les données sont isolées et décodées. Il relève également que conformément à l'arrêté royal du 12 août 1993 relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale, chaque IPSS est tenue d'instituer un service chargé de la sécurité de l'information, qui exerce notamment un rôle d'avis et de contrôle.

Il se réfère aussi aux mesures de sécurité prévues durant cette phase. En ce qui concerne l'accès, il insiste sur le devoir légal de discrétion et les garanties prévues par la loi BCSS et par l'arrêté royal du 12 août 1993. En ce qui concerne le codage, il renvoie à l'article 3 de la loi attaquée, qui dispose que des données ne peuvent être décodées que s'il y a un risque d'utilisation d'une adresse fictive. En ce qui concerne les mises à jour périodiques, il épingle la non-dérogation à l'article 4, § 1er, 3°, de la loi sur la protection de la vie privée.

Le Conseil des ministres reconnaît toutefois l'erreur matérielle commise lors de la rédaction du nouvel article 101/1, § 3, tel qu'il a été inséré par l'article 3, attaqué. Il souligne toutefois que les dispositions attaquées ne sauraient être comprises autrement que dans le sens où l'IPSS est la responsable de l'analyse des données relationnelles.

A.35. Enfin, il relève encore les garanties offertes lors du « constat » d'une fraude au domicile résultant du système « push ». Il affirme que le système a seulement une fonction de clignotant et que l'actionnement d'un clignotant ne conduit pas automatiquement au constat d'une fraude. Il souligne que la personne concernée a la possibilité d'invoquer tous éléments pour démontrer qu'il n'est nullement question d'une fraude au domicile. Conformément au Code pénal social, la personne concernée bénéficie en outre de toutes les garanties relatives aux droits de la défense, notamment le droit de s'entretenir avec un conseil avant d'être entendue par l'inspection sociale, et le droit d'accès au juge.

- B -

Quant au contexte des dispositions attaquées

B.1.1. La loi du 13 mai 2016 « modifiant la loi-programme (I) du 29 mars 2012 concernant le contrôle de l'abus d'adresses fictives par les bénéficiaires de prestations sociales, en vue d'introduire la transmission systématique de certaines données de consommation de sociétés de distribution et de gestionnaire de réseaux de distribution vers la BCSS améliorant le datamining et le datamatching dans la lutte contre la fraude sociale » (ci-après : la loi-programme (I) du 29 mars 2012), attaquée, règle, dans le cadre de la lutte contre la fraude sociale au domicile, premièrement l'échange de données entre, d'une part, les sociétés de distribution et les gestionnaires de réseaux de distribution et, d'autre part, les services publics et, deuxièmement, l'analyse d'une grande collection de données sociales. BCSS est l'abréviation de « Banque carrefour de la sécurité sociale ».

B.1.2. Par la loi attaquée, le législateur a voulu concrétiser son intention, clairement exprimée dans l'accord de gouvernement et dans les plans de politique successifs, de franchir une nouvelle étape dans la lutte contre la fraude sociale. Le législateur entendait lutter

progressivement et plus efficacement contre la fraude sociale au domicile en prévoyant de nouveaux instruments de contrôle concernant l'usage abusif d'adresses fictives (*Doc. parl.*, Chambre, 2011-2012, DOC 53-2081/017, p. 22; *Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, p. 8; *Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/005, p. 54).

B.1.3. Avant l'entrée en vigueur de la loi-programme (I) du 29 mars 2012, les bénéficiaires de prestations sociales étaient susceptibles de se voir réclamer les données de leur consommation d'eau, de gaz et d'électricité, le cas échéant, à des fins de contrôle. La loi-programme précitée a légalement permis à l'inspection sociale de réclamer ces données de consommation auprès des sociétés de distribution et des gestionnaires de réseaux de distribution (système « pull »).

Avant sa modification par l'article 2 attaqué, l'article 101 de la loi-programme (I) du 29 mars 2012 disposait :

« Si, dans le cadre d'une enquête, les inspecteurs sociaux présument sur la base d'autres éléments qu'un bénéficiaire utilise une adresse fictive afin de prétendre à des prestations sociales auxquelles il ne peut pas prétendre, ils peuvent demander les données de consommation d'eau, d'électricité et de gaz aux sociétés de distribution et aux gestionnaires de réseau de distribution.

Ces données de consommation peuvent être utilisées comme indication supplémentaire afin de démontrer qu'il s'agit d'une adresse fictive ».

Dans les travaux préparatoires, cet article fait l'objet du commentaire suivant :

« En exécution de la notification budgétaire 2012, la présente section vise à fournir aux autorités de contrôle une série de nouveaux instruments qui permettraient aux pouvoirs publics de renforcer la lutte contre la fraude aux allocations. Il veut être une initiative afin de mieux contrôler les allocations. L'objectif est d'arriver à ce qu'à chaque assuré social soit payée l'allocation correcte.

En concret, il est rendu possible pour les inspecteur[s] sociaux de demander aux société[s] de distribution et aux gestionnaires de réseau de distribution les données de consommation d'eau, d'électricité et de gaz des personnes qui ont droit à une prestation sociale.

Celles-ci sont obligées à répondre à une telle demande en donnant les données » (*Doc. parl.*, Chambre, 2011-2012, DOC 53-2081/001, p. 71).

« Il est prévu de permettre aux inspecteurs sociaux de demander les données de consommation (d'eau, d'électricité et de gaz) aux sociétés de distribution et aux gestionnaires de réseau de distribution s'ils présument, sur la base d'autres éléments, que des bénéficiaires de prestations sociales commettent une fraude au domicile. Les sociétés de distribution et les gestionnaires de réseau de distribution, qui ne répondent pas toujours, aujourd'hui, à toutes les demandes d'informations, seront désormais obligés de répondre à ces demandes et de fournir les données demandées. Les informations fournies pourront constituer un indice supplémentaire d'abus mais pas une preuve concluante.

Cette mesure est une première étape mais ne réglera pas intégralement ce problème. D'autres réformes seront nécessaires à l'avenir pour lutter contre la fraude au domicile » (*Doc. parl.*, Chambre, 2011-2012, DOC 53-2081/017, p. 22).

B.1.4. Ce système « pull » n'a jamais été mis en pratique (*Doc. parl.*, Chambre, 2015-2016, DOC 54-0020/063, p. 14).

B.2.1. La loi attaquée remplace le système « pull », précité, par un système « push » et prévoit de nouvelles possibilités de « data mining » en matière de lutte contre la fraude sociale au domicile.

B.2.2. En ce qui concerne le passage au système « push » d'échange de données, les travaux préparatoires mentionnent ce qui suit :

« Le système actuel, appelé système ' pull ', dans lequel les sociétés de distribution et les gestionnaires de réseaux de distribution doivent transmettre ces données de consommation à la demande des services d'inspections, est converti en un système ' push '. Cela signifie que les sociétés de distribution et les gestionnaires de réseaux de distribution enverront dorénavant automatiquement et électroniquement à la [Banque-carrefour de la Sécurité Sociale; ci-après : la BCSS] les données de consommation visées. Ces données serviront d'indicateurs supplémentaires afin de permettre aux services d'inspection sociale de mieux détecter [la] fraude au domicile. Concrètement, les données de consommation seront utilisées par le BCSS pour le datamatching et, dans une phase ultérieure, comme des indicateurs supplémentaires pour le datamining. De cette manière le gouvernement rencontre le point 31 de l'avis de la Commission de la protection de la vie privée (CPVP) de ne pas transmettre aux sociétés de distribution et aux gestionnaires de réseaux de distribution, des données supplémentaires ni quant au statut social de la personne concernée, ni sur la composition de ménage » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, pp. 5-6).

En ce qui concerne la transition vers le nouveau système, il est encore mentionné ce qui suit :

« Le système ' pull ' introduit en 2012 était un pas dans la bonne direction. Il est nécessaire à présent de passer au système ' push ', plus efficace, tout d'abord dans le cadre

d'une phase de test devant permettre d'améliorer la méthode » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/005, p. 54).

Dans les travaux préparatoires, la plus-value du système « push » fait ensuite l'objet du commentaire suivant :

« La plus-value de ce changement de politique se trouve dans le fait que le push d'une consommation extrêmement basse ou extrêmement haute, dépendant de la composition de ménage, permet d'activer un déclencheur d'alerte dans les cas où il n'y a pas encore une présomption de fraude. C'est là aussi que se trouve la plus-value du datamining: rendre les contrôles plus efficaces et plus focalisés. Dans le système ' pull ' cette plus-value est très limitée puisqu'on demande des données supplémentaires sur base d'un dossier concret avec présomption de fraude » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, p. 6).

B.2.3.1. En ce qui concerne les objectifs poursuivis par le législateur, les travaux préparatoires mentionnent ce qui suit :

« Conformément à la notification budgétaire approuvée par le Conseil des ministres du 3 avril 2015 (pages 39-40), le présent projet de loi a pour objectif de rendre possible la transmission systématique des données de consommation des sociétés de distribution vers la Banque Carrefour de la Sécurité Sociale. Cela devra renforcer le contrôle sur l'attribution correcte des prestations sociales.

On prend de plus en plus conscience de l'hypothèque que la fraude aux allocations fait peser sur notre sécurité sociale. Or, pour rester viable, celle-ci a besoin d'une large assise sociale fondée sur la solidarité.

La fraude aux allocations touche notre système de sécurité sociale en plein cœur. Elle mine en effet un de ses fondements, à savoir la solidarité. Ce principe constitue un des fondements de notre système.

De nombreux citoyens paient honnêtement leurs cotisations et perçoivent leurs allocations en toute régularité. Seul un groupe déterminé ne respecte pas les règles et lèse ainsi les autres citoyens qui, eux, contribuent correctement au régime de sécurité sociale et qui en bénéficient lorsqu'ils y ont droit.

Dans différentes branches de la sécurité sociale, comme le chômage et l'assurance maladie-invalidité, certaines prestations sont en effet octroyées avec majoration en fonction de la situation familiale de l'assuré social.

Les domiciliations fictives constituent un mécanisme de fraude qui en découle, vu que l'assuré social ne déclare pas, sciemment, son véritable domicile et/ou sa situation familiale afin d'obtenir de façon illicite une allocation plus élevée que celle à laquelle il a droit.

Compte tenu de son impact, la fraude sociale liée à la domiciliation fictive est un phénomène auquel les services d'inspection sont particulièrement attentifs.

Dans le cadre d'un renforcement de la lutte contre la fraude sociale, des mesures externes (renforcement de la collaboration avec les magistrats, la police et les autres institutions publiques de sécurité sociale) ainsi que des mesures internes (établissement de nouvelles procédures administratives) ont été élaborées et mises en application.

Il a également été décidé de prévoir une stratégie globale de lutte contre les domiciliations fictives, impliquant toutes les institutions de sécurité sociale et les organismes octroyant des avantages sociaux, en définissant des lignes directrices pour la recherche et la poursuite tout en respectant la vie privée.

Le Collège des Procureurs généraux a édicté une circulaire sur le phénomène de la fraude sociale par le biais d'inscriptions fictives. Cette circulaire du Collège des Procureurs généraux (COLL. PG 17/2013) et son vademecum sont entrés en vigueur le 2 septembre 2013 » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, pp. 4-5).

B.2.3.2. Il en ressort que le législateur, fort de l'idée que la fraude aux allocations mine la solidarité comme fondement de la sécurité sociale, a considéré la lutte contre la fraude sociale comme une préoccupation sociétale importante. Il a déjà pris plusieurs mesures dans le but de renforcer la lutte contre la fraude sociale. Par la réglementation attaquée, il se concentre en particulier sur la fraude sociale au domicile, eu égard au lien étroit entre le montant des prestations sociales, la situation de domicile et la situation familiale.

B.3.1. Le législateur vise donc à renforcer la lutte contre la fraude sociale au domicile en recourant à des techniques de traitement modernes sans que les données de consommation sélectionnées et transmises, qu'on appelle « signaux d'alerte », soient déterminantes pour établir si un bénéficiaire de prestations sociales a utilisé une adresse fictive.

La loi attaquée tend donc à fournir aux services publics, en l'espèce les inspecteurs sociaux et les institutions publiques de sécurité sociale (ci-après : les IPSS), des instruments plus efficaces et performants pour exécuter leurs tâches légales en matière de sécurité sociale. Les inspecteurs sociaux sont les fonctionnaires qui sont sous l'autorité des ministres ayant dans leurs attributions l'emploi et le travail, la sécurité sociale, les affaires sociales et la santé publique, ou qui relèvent des institutions publiques qui en dépendent, et qui sont chargés de veiller au respect des lois sociales (article 16, 1°, du Code pénal social). Les IPSS sont les services publics fédéraux chargés d'appliquer la législation relative à la sécurité sociale.

B.3.2. Le législateur a notamment considéré, entre autres en raison des possibilités qu'offrent les techniques de « profilage », qui s'appuient sur le « data warehousing », le « data matching » et le « data mining », que, d'une part, la mise automatique et systématique à disposition des services publics mentionnés en B.3.1 des adresses et données de consommation d'eau, de gaz et d'électricité sélectionnées et, d'autre part, l'analyse des données agrégées disponibles et la recherche, par ces services, d'indicateurs de risques dans ces données, sont des instruments utiles dans la lutte contre la fraude sociale au domicile.

B.3.3. Le « profilage » se déroule en trois étapes distinctes, au cours desquelles on recherche ou on se base sur des patrons et modèles (les « profils ») : une première étape de collecte et de conservation à grande échelle (« data warehousing ») d'informations au sujet des comportements et caractéristiques des individus; une deuxième et une troisième étape d'analyse et d'exploitation de ces données permettant de faire des corrélations entre certains comportements et certaines caractéristiques, et au cours desquelles sont déduites de ces données, à partir des corrélations précitées, de nouvelles caractéristiques ou variables comportementales inconnues ou cachées (existantes, futures ou antérieures « data mining »).

B.3.4. Cette technique de « profilage » tend donc à détecter, à partir d'un profil, un ensemble de particularités qui caractérisent une catégorie de personnes (p. ex. les fraudeurs), à identifier un individu afin, d'une part, de prendre des décisions à son égard (p. ex. lancer une enquête), et, d'autre part, d'analyser ou de prévoir ses préférences, comportements et attitudes personnels (point 1, d. et e., de la recommandation (2010)13 du Comité des ministres aux Etats membres du 23 novembre 2010 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage (ci-après : la recommandation (2010)13).

B.3.5. Lorsqu'on recourt à cette technique, il est toutefois 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, et notamment d'arriver à des résultats faussement positifs ou faussement négatifs, ce qui nécessite de faire une évaluation et un suivi permanents des critères (voy. Commission de la protection de la vie privée, avis 24/2015, p. 7; avis 05/2016, p. 6).

B.4. Il ressort des travaux préparatoires de la loi attaquée que le législateur a concrétisé son objectif en conférant un fondement légal au contrôle renforcé de la fraude sociale au domicile par un échange de données automatisé entre les prestataires de services et les services publics et aux techniques modernes de recherche dans de vastes banques de données (« data warehousing »), comme le « data matching » et le « data mining », sans porter atteinte aux exigences fixées en matière de protection de la vie privée (voy. article 104 de la loi-programme (I) du 29 mars 2012) :

« Pour cette raison, le projet prévoit une base légale permettant de transmettre électroniquement à la Banque-Carrefour de la Sécurité Sociale (BCSS) certaines données de consommation d'eau, de gaz et d'électricité et les adresses de certains particuliers » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, p. 5).

« La Commission [de la protection de la vie privée] a recommandé une base légale générale similaire pour le recours au ' datamining ' et au ' datamatching ' au moyen des banques de données pertinentes, tel qu'utilisées, entre autres, par la plateforme OASIS. Bien que la Commission indique clairement que cette recommandation dépasse le cadre du dossier actuel, l'ajout de ce paragraphe permet déjà de satisfaire à cette recommandation de la Commission pour ce qui concerne les données énergétiques et une base légale est établie à cet effet pour le datamining » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/004, p. 9).

« Cette méthode permettra, comme c'est déjà le cas aux Pays-Bas, de vérifier, de manière automatique et en respectant la vie privée, si les données de consommation déclarées correspondent ou non aux données de domiciliation. Ce croisement de données pourra déclencher une alerte qui nécessitera une enquête plus approfondie. Les données énergétiques sont déjà effectivement utilisées aujourd'hui dans la lutte contre les logements inoccupés, à Bruxelles, par exemple.

Afin de mettre tout ceci en œuvre, la législation existante, reprise aux articles 100 à 105 inclus de la loi-programme du 29 mars 2012, est modifiée. Cette loi contient déjà une disposition qui rend applicable la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Cette disposition est évidemment maintenue dans le nouveau système » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, p. 6).

B.5.1. Les mesures devant permettre au législateur de réaliser son objectif sont contenues dans les articles 2 et 3 de la loi attaquée.

B.5.2. L'article 2 de la loi attaquée prévoit un système « push » - sur plusieurs étapes au but très spécifique - qui permet de transmettre électroniquement certaines données de consommation d'eau, de gaz et d'électricité et les adresses de certains particuliers à la BCSS,

qui se charge de les filtrer et de les croiser (« data matching ») avec d'autres données en vue de les communiquer aux IPSS et aux inspecteurs sociaux intéressés, dans le but de renforcer la performance et l'efficacité de la lutte contre la fraude aux allocations (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, p. 5).

Lors d'une première étape, les sociétés de distribution et les gestionnaires de réseaux de distribution sont tenus de collecter des données de consommation et des adresses. Ils doivent ensuite transmettre certaines de ces données à la BCSS, au minimum une fois par an. Ces données sont sélectionnées lorsqu'un écart d'au moins 80 % par rapport à la consommation moyenne correspondant à la composition de ménage officiellement communiquée est constaté (article 101, § 1er, alinéa 1er, de la loi-programme (I) du 29 mars 2012, tel qu'il a été remplacé par l'article 2 de la loi attaquée). Les types de familles et la consommation moyenne par type de famille sont annuellement fixés par le comité de gestion de la BCSS, en concertation avec les sociétés de distribution et les gestionnaires de réseaux de distribution (article 101, § 1er, alinéa 2, de la loi-programme (I) du 29 mars 2012, tel qu'il a été remplacé par l'article 2 de la loi attaquée).

Lors d'une deuxième étape, les données ainsi collectées et obtenues par la BCSS sont transmises, après avoir été croisées avec les données enregistrées au Registre national, pour déceler qui habite aux différentes adresses communiquées aux IPSS et aux inspecteurs sociaux, à condition que les institutions visées octroient une prestation sociale ou exercent une quelconque forme de contrôle du respect des lois octroyant un avantage (« data matching »; article 101, § 1er, alinéa 3, de la loi-programme (I) du 29 mars 2012, tel qu'il a été remplacé par l'article 2 de la loi attaquée).

Ensuite, les inspecteurs sociaux ou les IPSS peuvent contrôler, après autorisation du comité sectoriel de la sécurité sociale et de la santé, sur la base des données obtenues, en combinaison avec d'autres données (à caractère personnel) issues des banques de données sociales, de la BCSS et du Registre national, si une prestation sociale est allouée sur la base d'une adresse fictive (« data mining »; article 101, § 1er, alinéa 3, de la loi-programme (I) du 29 mars 2012, tel qu'il a été remplacé par l'article 2 de la loi attaquée).

Toutefois, les données de consommation et les adresses communiquées ne peuvent en soi amener à conclure que le bénéficiaire d'une prestation sociale s'est rendu coupable de fraude

sociale au domicile (article 102 de la loi-programme (I) du 29 mars 2012, tel qu'il a été remplacé par l'article 4 de la loi attaquée).

B.5.3. L'article 3 autorise par ailleurs les IPSS à rechercher des corrélations et des indicateurs de risque en matière de fraude sociale au domicile dans les données, agrégées, issues de banques de données sociales pertinentes (« data mining »).

Au cours de cette troisième étape, les IPSS, dont relèvent aussi les inspecteurs sociaux, peuvent procéder au regroupement des données de consommation et des adresses recueillies avec d'autres données dont elles disposent, pour analyser des données relationnelles qui doivent permettre aux services concernés de réaliser des contrôles ciblés, sur la base d'indicateurs de risque d'octroi d'une aide calculée sur la base d'une adresse fictive (article 101/1 de la loi-programme (I) du 29 mars 2012, tel qu'il a été inséré par l'article 3 de la loi attaquée). Cette analyse se fait à partir de données codées qui ne peuvent être décodées qu'après avoir été isolées, lorsqu'une analyse indique le risque d'une utilisation d'une adresse fictive.

B.6. Le législateur a en outre choisi de confier la fixation des règles d'exécution relatives au système instauré au comité de gestion de la BCSS. Dans les travaux préparatoires, cette délégation est commentée en ces termes :

« Néanmoins, il est également prévu que non pas le Roi, mais le comité de gestion de la Banque-Carrefour de la sécurité sociale devra fixer la consommation moyenne par type de famille. Le comité de gestion devra le faire en concertation avec les acteurs du terrain, à savoir les sociétés de distribution et les gestionnaires de réseaux de distribution. Selon le gouvernement cette approche permet de fixer le seuil le plus adéquat et, si nécessaire, de l'adapter rapidement aux circonstances changeantes sur le terrain afin de lutter efficacement contre la fraude au domicile. En effet, la fraude au domicile est une donnée évolutive et en outre le gouvernement ne veut en aucun cas toucher aux ayants droit de bonne foi. Cette préoccupation est rencontrée par la possibilité d'une délégation prévu[e] au comité de gestion » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, pp. 7-8).

Quant aux dispositions attaquées

B.7.1.1. L'article 2 de la loi attaquée remplace l'article 101 de la loi-programme (I) du 29 mars 2012 par ce qui suit :

« § 1er. En fonction de la périodicité de leur collecte de données et au minimum une fois par année calendrier, les sociétés de distribution et les gestionnaires de réseaux de distribution transmettent électroniquement à la Banque Carrefour de la Sécurité Sociale certaines données de consommation et les adresses de certains de leurs clients privés. Il s'agit des données sélectionnées par les sociétés de distribution et les gestionnaires de réseaux de distribution parce que la consommation du client privé s'écarte d'au moins 80 % vers le haut ou vers le bas d'une consommation moyenne en fonction de la composition de ménage officiellement communiquée.

Les types de famille et la consommation moyenne par type de famille sont annuellement fixés par le comité de gestion de la Banque Carrefour de la Sécurité Sociale en concertation avec les sociétés de distribution et les gestionnaires de réseaux de distribution.

La Banque Carrefour de la Sécurité Sociale transmet les données visées à l'alinéa 1er, après croisement avec les données enregistrées au Registre national, visé par la loi du 8 août 1983 organisant un registre national des personnes physiques, aux institutions publiques de sécurité sociale et aux inspecteurs sociaux à condition que les institutions visées octroient au bénéficiaire auquel ces données ont trait une prestation sociale, soit de la sécurité sociale, soit d'un régime d'aide sociale, ou d'autres avantages accordés par les réglementations sur lesquelles les inspecteurs sociaux exercent la surveillance. Cela doit leur permettre de contrôler, après autorisation du comité sectoriel de la sécurité sociale et de la santé, en combinaison avec d'autres données sociales et des données sociales à caractère personnel qui sont disponibles dans le réseau, telles que visées à la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la Sécurité Sociale, si la prestation sociale est octroyée sur la base d'une adresse fictive.

§ 2. Pour les traitements de données visés au § 1er, il est désigné comme responsable de traitement tel que visé à l'article 1er, § 4, 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, la Banque Carrefour de la Sécurité Sociale ».

B.7.1.2. En ce qui concerne le premier paragraphe de la disposition nouvelle, les travaux préparatoires mentionnent :

« Cet article oblige les sociétés de distribution et les gestionnaires de réseaux de distribution à transmettre électroniquement à la Banque Carrefour de la Sécurité Sociale, en fonction de la périodicité de leur collecte des données et au minimum une fois par année calendrier, certaines données de consommation et les adresses de certains de leurs clients privés. Ceci signifie donc que les données font désormais l'objet d'un système ' push '. Cela doit se faire donc au moins une fois par année, mais si cela est possible pour certaines sociétés de distribution et gestionnaires de réseaux de distribution, les données pourront également

être transmises plusieurs fois par année. Il s'agit des données sélectionnées par les sociétés de distribution et les gestionnaires de réseaux parce qu'elles s'écartent d'au moins 80 % vers le haut ou vers le bas d'une consommation moyenne en fonction de la composition de ménage officiellement communiquée. Les types de famille et la consommation moyenne par type de famille sont annuellement fixés par le comité de gestion de la Banque-Carrefour de la sécurité sociale en concertation avec les sociétés de distribution et les gestionnaires de réseaux de distribution.

Dans l'avant-projet de loi il a été prévu que la communication des données de consommation se ferait sur base de certains seuils de consommation, qui peuvent indiquer une consommation inférieure ou supérieure en fonction de la composition de ménage officiellement communiquée. Ces seuils seraient fixés par le Roi par un arrêté royal délibéré en Conseil des ministres. Cependant, le Conseil d'État a remarqué dans le point 8.2. de son avis que cette délégation au Roi est trop large. Vu cette remarque le gouvernement a jugé souhaitable d'en effet prévoir déjà une limitation dans la loi même. Pour cette raison la règle de 80 % est inscrite dans la loi même. Néanmoins, il est également prévu que non pas le Roi, mais le comité de gestion de la Banque-Carrefour de la sécurité sociale devra fixer la consommation moyenne par type de famille. Le comité de gestion devra le faire en concertation avec les acteurs du terrain, à savoir les sociétés de distribution et les gestionnaires de réseaux de distribution. Selon le gouvernement cette approche permet de fixer le seuil le plus adéquat et, si nécessaire, de l'adapter rapidement aux circonstances changeantes sur le terrain afin de lutter efficacement contre la fraude au domicile. En effet, la fraude au domicile est une donnée évolutive et en outre le gouvernement ne veut en aucun cas toucher aux ayants droit de bonne foi. Cette préoccupation est rencontrée par la possibilité d'une délégation prévu[e] au comité de gestion.

En outre, d'après la CPVP, il convient de mieux justifier le passage d'un modèle ' pull ' à un modèle ' push '. Etant donné que différentes institutions publiques de sécurité sociale (IPSS) octroient des prestations qui varient en fonction de la composition du ménage, il est important pour elles de pouvoir contrôler le mieux possible si la composition du ménage déclarée est bien correcte. Pour l'instant, les services d'inspection vérifient cela au moyen, entre autres, de contrôles sur place au domicile déclaré ou en demandant les données de consommation auprès de l'assuré social même ou des sociétés de distribution ou des gestionnaires de réseau de distribution. Le modèle push proposé est destiné à renforcer ces instruments existants et à rendre le contrôle plus efficace et plus performant. Lors des discussions au Conseil National du Travail, l'Office national de l'Emploi a par exemple indiqué que ce système permettra en effet à leurs inspecteurs sociaux d'exercer un contrôle plus ciblé et plus efficace du respect des règles de la réglementation du chômage.

D'autre part, la CPVP se pose également la question de savoir pourquoi on vise à la fois une consommation trop faible et une consommation trop élevée. Compte tenu de ce qui précède, il est logique que les deux extrêmes soient pris en considération, car il est possible que chacun des partenaires d'un couple bénéficie […] d'une allocation. Afin d'augmenter l'allocation de chacun d'entre eux, ils déclarent chacun d'être isolé. Pour le prouver, ils ont une résidence séparée. Cela signifie qu'ils bénéficient tous les deux d'une allocation en qualité d'isolé. Celle-ci est évidemment plus élevée qu'une allocation en qualité de cohabitant. Cependant, dans les faits, ils vivent encore ensemble. Dans un des deux domiciles la consommation sera en principe plus faible que la consommation moyenne d'un isolé. Dans l'autre domicile, elle sera en principe plus élevée. Grâce à cette mesure, ces deux types de fraudes peuvent être détectés.

En outre, la finalité de cette obligation est précisée. Ces données doivent permettre aux inspecteurs sociaux de contrôler si les prestations de sécurité sociale ou d'assistance sociale payées ont été octroyées à juste titre.

A cette fin, ces données doivent être combinées avec d'autres données dont les services compétents disposent ou auxquelles ils ont accès.

Afin d'avoir accès à ces données de consommation et afin de pouvoir les combiner avec les autres données, les services intéressés doivent, comme toujours, demander une autorisation du Comité sectoriel de la Sécurité sociale et de la Santé.

Suite à la remarque 9.4 du Conseil d'Etat le texte a été adapté afin de mettre en évidence que les données de consommation divergentes sont uniquement communiquées par la BCSS au cas où les personnes concernées touchent des allocations des institutions concernées.

Cette adaptation permet de répondre d'emblée à la remarque de la CPVP selon laquelle les sociétés privées (sociétés de distribution ou gestionnaires de réseau de distribution) ne peuvent pas recevoir des informations complémentaires sur l'assuré social, venant de l'inspection sociale ou du registre national. Il s'agit très clairement d'une circulation de données à sens unique. Les sociétés privées doivent fournir des informations. Elles n'en reçoivent pas » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, pp. 7-9).

En ce qui concerne le second paragraphe, les travaux préparatoires mentionnent :

« Dans ses avis des 17 juin 2015 et 3 février 2016, la Commission vie privée souligne que le responsable de traitement n'est pas désigné explicitement dans le projet. Etant donné que de nombreux acteurs seront associés à la lutte contre la fraude sociale visée par le projet de loi (gestionnaires de réseau de distribution, BCSS, inspection sociale, sous-traitants éventuels…), la question se posera tôt ou tard de savoir qui est le responsable ou le sous-traitant du ou des différents traitements visés par le Projet. Etant donné que pour tous ces traitements, les droits et obligations actuels et futurs doivent être respectés par tout responsable aux termes de la LVP et du RGPD, il est important d'apporter des précisions à cet égard. La Commission vie privée indique dans son avis que cette désignation peut également avoir lieu d'une manière précise dans les autorisations d'échange de données. Afin d'accroître la transparence, le responsable de traitement sera également désigné clairement dans la loi. En ce qui concerne le ' datamatching ', la ' Banque-Carrefour de la Sécurité Sociale ' est désignée comme responsable de traitement » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/004, p. 7).

B.7.2.1. L'article 3 de la loi attaquée insère, dans la loi-programme (I) du 29 mars 2012, un article 101/1 (nouveau), qui dispose :

« § 1er. Chaque institution publique de sécurité sociale (IPSS) peut procéder à l'agrégation des données recueillies en application de l'article 101 avec d'autres données dont les IPSS disposent, pour effectuer des analyses sur des données relationnelles qui doivent permettre à ses services de réaliser des contrôles ciblés sur la base d'indicateurs de risque

d'octroi d'une aide calculée sur la base d'une adresse fictive. L'analyse se fait à partir de données codées. Les données indiquant un risque d'utilisation d'une adresse fictive sont isolées et décodées.

§ 2. Toute catégorie de données communiquée dans le cadre de l'article 101, § 1er, à un IPSS fait l'objet d'une autorisation d'un comité sectoriel institué au sein de la Commission de la protection de la vie privée. L'autorisation fixe les conditions relatives au délai de conservation des données codées et décodées.

§ 3. Les analyses sur les données relationnelles visées à l'article 101, § 1er, ont pour responsable de traitement, tel que visé à l'article 1er, § 4, 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, l'IPSS qui procède à l'analyse sur les données relationnelles ».

B.7.2.2. En ce qui concerne le premier paragraphe de cette disposition, les travaux préparatoires mentionnent :

« Dans son avis du 3 février 2016, la Commission vie privée fait référence à l'article 5, § 1er, 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, qui dispose que :

' § 1er. Le Service public fédéral Finances peut procéder également à l'agrégation des données recueillies en application de l'article 3 en vue de la création d'un datawarehouse qui doit permettre à ses services d'une part, de réaliser des contrôles ciblés sur la base d'indicateurs de risque et d'autre part, d'effectuer des analyses sur des données relationnelles provenant des différentes administrations et, ou services du Service public fédéral Finances. ' La Commission a recommandé une base légale générale similaire pour le recours au ' datamining ' et au ' datamatching ' au moyen des banques de données pertinentes, tel qu'utilisées, entre autres, par la plateforme OASIS. Bien que la Commission indique clairement que cette recommandation dépasse le cadre du dossier actuel, l'ajout de ce paragraphe permet déjà de satisfaire à cette recommandation de la Commission pour ce qui concerne les données énergétiques et une base légale est établie à cet effet pour le datamining » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/004, p. 9).

En ce qui concerne le deuxième paragraphe, il est dit :

« Dans ses avis des 17 juin 2015 et 3 février 2016, la Commission vie privée pose la question d'une durée de conservation des données adaptée, compte tenu de l'article 4, § 1er, 4°, de la loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (LVP). La Commission indique que la définition d'une durée de conservation peut avoir lieu d'une manière précise dans les autorisations d'échange de données. Au paragraphe 2, il est défini que ces autorisations doivent préciser des durées de conservation pour des données codées et décodées » (*ibid.*).

Le troisième paragraphe est commenté en ces termes :

« En ce qui concerne le ‘ datamining ’ ‘ l’IPSS qui procède à l’analyse sur les données relationnelles ’ est désignée comme responsable de traitement » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/004, p. 10).

B.7.3.1. L’article 4 de la loi attaquée remplace l’article 102 de la loi-programme (I) du 29 mars 2012 par ce qui suit :

« Les données visées à l’article 101 peuvent uniquement être utilisées comme indication supplémentaire afin de décider si un bénéficiaire utilise une adresse fictive ».

B.7.3.2. Les travaux préparatoires de cette disposition mentionnent :

« Cet article dispose que les données peuvent uniquement être utilisées comme indication supplémentaire afin de constater si un bénéficiaire utilise une adresse fictive.

En effet, il ne s’agit pas de conclure qu’il y a fraude en se basant uniquement sur les données de consommation. Ces données elles-mêmes ne sont pas suffisamment probantes à cet effet » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, p. 9).

B.7.4. Dans l’article 103 de la loi-programme (I) du 29 mars 2012, l’article 5 de la loi attaquée remplace le mot « demander » par le mot « utiliser ».

B.7.5.1. L’article 6 de la loi attaquée remplace l’article 105 de la loi-programme (I) du 29 mars 2012 par ce qui suit :

« Le comité de gestion de la Banque Carrefour de la Sécurité Sociale détermine les modalités, entre autres la structure et le contenu des messages avec lesquels les données sont transmises, la façon selon laquelle et le moment auquel les données de consommation et d’adresses sont transmises ».

B.7.5.2. Les travaux préparatoires de cette disposition mentionnent :

« Cet article prévoit une délégation au Comité de gestion de la Banque Carrefour de la Sécurité Sociale.

Le comité de gestion devra déterminer les modalités pratiques d’application de la mesure. Il s’agit, entre autres, de la structure et du contenu des messages, de la façon dont et le moment auquel les données de consommation et les adresses doivent être transmises. Une telle délégation au comité de gestion n’est pas neuve et est justifiée par le fait qu’il s’agit

souvent d'aspects techniques pour lesquels une réaction rapide est nécessaire, compte tenu d'un environnement informatique qui évolue rapidement » (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1554/001, pp. 9-10).

Quant à la recevabilité du recours

B.8.1. Les griefs soulevés par la partie requérante étant exclusivement dirigés contre les articles 2, 3 et 4 de la loi attaquée, le recours est seulement recevable en ce qu'il est dirigé contre ces articles.

B.8.2.1. Le Conseil des ministres conteste la recevabilité de la plupart des griefs formulés dans le moyen unique au motif qu'ils ne seraient pas suffisamment développés ou qu'ils seraient dénués de pertinence. En outre, il souligne à plusieurs reprises qu'un des griefs formulés serait totalement ou partiellement irrecevable parce que la Cour n'est pas compétente pour exercer un contrôle direct au regard de dispositions conventionnelles, de dispositions législatives (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 « loi relative à la protection de la vie privée »), d'actes législatifs de l'Union européenne (la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après : la « directive 95/46/CE ») et le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)) et des principes généraux de nécessité, de subsidiarité, de proportionnalité, de transparence, de limitation de conservation, d'obligation de justification, d'intégrité et de sécurité.

B.8.2.2. La Cour est compétente pour contrôler des normes de nature législative au regard des règles répartitrices de compétence entre l'Etat fédéral, les communautés et les régions, ainsi qu'au regard des articles du titre II (« Des Belges et de leurs droits ») et des articles 143, § 1er, 170, 172 et 191 de la Constitution.

Tous les griefs sont pris de la violation d'une ou de plusieurs règles dont la Cour garantit le respect.

Dans la mesure où la partie requérante invoque en outre des dispositions conventionnelles, des actes législatifs de l'Union européenne, des dispositions législatives et des principes généraux, la Cour ne les examine qu'en tant que la partie requérante dénonce la violation des dispositions constitutionnelles précitées, combinées avec les dispositions, actes et principes visés. Dans cette mesure, les griefs sont recevables.

B.8.3. Pour satisfaire aux exigences de l'article 6 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, les moyens de la requête doivent faire connaître, parmi les règles dont la Cour garantit le respect, non seulement celles qui seraient violées, mais aussi les dispositions qui violeraient ces règles, et exposer en quoi ces règles auraient été transgressées par les dispositions visées.

La Cour examine les griefs formulés dans le moyen unique, dans la mesure où ils satisfont aux exigences précitées.

B.8.4. Les exceptions sont rejetées.

Quant au droit au respect de la vie privée

B.9. Le moyen unique est principalement pris, mais pas exclusivement, de la violation du droit au respect de la vie privée, tel qu'il est garanti par l'article 22 de la Constitution, combiné avec l'article 8 de la Convention européenne des droits de l'homme, avec l'article 17 du Pacte international relatif aux droits civils et politiques et avec les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

B.10.1. L'article 22 de la Constitution dispose :

« Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi.

La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit ».

B.10.2. L'article 8 de la Convention européenne des droits de l'homme dispose :

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

B.10.3. Le Constituant a recherché la plus grande concordance possible entre l'article 22 de la Constitution et l'article 8 de la Convention européenne précitée (*Doc. parl.*, Chambre, 1992-1993, n° 997/5, p. 2).

La portée de cet article 8 est analogue à celle de la disposition constitutionnelle précitée, de sorte que les garanties que fournissent ces deux dispositions forment un ensemble indissociable.

B.10.4. L'article 17 du Pacte international relatif aux droits civils et politiques dispose :

« 1. Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.

2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ».

B.10.5. Les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne disposent :

« Art. 7. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications ».

« Art. 8. 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

Dans le contrôle qu'elle exerce au regard des articles 7 et 8 précités, la Cour doit prendre en compte l'article 52, paragraphe 1, de la Charte, qui dispose :

« Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ».

B.11. 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. La jurisprudence de la Cour européenne des droits de l'homme fait apparaître que de la protection de ce droit relèvent notamment les données et informations personnelles suivantes : le nom, l'adresse, les activités professionnelles, les relations personnelles, les empreintes digitales, les images filmées, les photographies, les communications, les données ADN, les données judiciaires (condamnations ou inculpations), les données financières et les informations concernant des biens (voy. notamment CEDH, 23 mars 1987, *Leander* c. Suède, §§ 47-48; grande chambre, 4 décembre 2008, *S. et Marper* c. Royaume-Uni, §§ 66-68; 17 décembre 2009, *B.B.* c. France, § 57; 10 février 2011, *Dimitrov-Kazakov* c. Bulgarie, §§ 29-31; 18 octobre 2011, *Khelili* c. Suisse, §§ 55-57; 9 octobre 2012, *Alkaya* c. Turquie, § 29; 18 avril 2013, *M.K.* c. France, § 26; 18 septembre 2014, *Brunet* c. France, § 31).

B.12. Les droits que garantissent l'article 22 de la Constitution et l'article 8 de la Convention européenne des droits de l'homme ne sont toutefois pas absolus.

Ils n'excluent pas toute ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée mais exigent que cette ingérence 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 (CEDH, 27 octobre 1994, *Kroon et autres* c. Pays-Bas, § 31; grande chambre, 12 octobre 2013, *Söderman* c. Suède, § 78).

B.13.1. 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.

B.13.2. 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 éclairés - prévoir, à un degré raisonnable, dans les circonstances de la cause, les conséquences d'un acte déterminé (CEDH, grande chambre, 4 mai 2000, *Rotaru* c. Roumanie, § 55; grande chambre, 17 février 2004, *Maestri* c. Italie, § 30). 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 (CEDH, grande chambre, 12 juin 2014, *Fernández Martínez* c. Espagne, § 117).

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 juridictionnel effectif, d'autre part (CEDH, grande chambre, 4 mai 2000, *Rotaru* c. Roumanie, § 55; 6 juin 2006, *Segerstedt-Wiberg* c. Suède, § 76; 4 juillet 2006, *Lupsa* c. Roumanie, § 34).

B.13.3. Il découle dès lors de l'article 8 de la Convention européenne des droits de l'homme 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 (CEDH, grande chambre, 4 mai 2000, *Rotaru* c. Roumanie, § 57; grande chambre, 12 janvier 2010, *S. et Marper* c. Royaume-Uni, § 99).

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 (CEDH, grande chambre, 12 janvier 2010, *S. et Marper* c. Royaume-Uni, §§ 95 et 96). Ainsi, la Cour européenne des droits de l'homme 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 (CEDH, 26 mars 1987, *Leander* c. Suède, § 51; 4 juillet 2006, *Lupsa* c. Roumanie, § 33).

B.14.1. 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 répondre à un besoin social impérieux dans une société démocratique et être proportionnée au but légitime poursuivi.

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.

B.14.2. Pour juger de cet équilibre, la Cour européenne des droits de l'homme tient compte notamment des dispositions de la Convention du Conseil de l'Europe du 28 janvier 1981 « pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel » (ci-après : la « Convention n° 108 »)(CEDH, 25 février 1997, *Z* c. Finlande, § 95; grande chambre, 12 janvier 2010, *S. et Marper* c. Royaume-Uni, § 103).

Cette Convention contient, entre autres, les principes relatifs au traitement de données à caractère personnel : licéité, loyauté, transparence, limitation des finalités, proportionnalité, exactitude, limitation de la conservation, intégrité et confidentialité, et responsabilité.

Pour interpréter ces principes, il y a lieu, en l'espèce, de tenir compte en particulier du contenu de la recommandation (2010)13.

B.14.3. Une ingérence dans l'exercice du droit au respect de la vie privée par un traitement de données à caractère personnel, en l'occurrence par un accès et par l'utilisation par les services publics de certaines données personnelles au moyen de techniques particulières (CEDH, 23 mars 1987, *Leander* c. Suède, § 48; grande chambre, 4 mai 2000, *Rotaru* c. Roumanie, § 46; CJUE, grande chambre, 8 avril 2014, C-293/12, *Digital Rights Ireland Ltd*, et C-594/12, *Kärntner Landesregierung e.a.*) doit donc reposer sur une justification raisonnable et être proportionnée aux buts poursuivis par le législateur.

B.14.4. 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 mentionnées en B.13.2.

Pour juger du caractère proportionné de mesures relatives au traitement de données à caractère personnel, il convient dès lors 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 (CEDH, grande chambre, 4 mai 2000, *Rotaru* c. Roumanie, § 59; décision, 29 juin 2006, *Weber et Saravia* c. Allemagne, § 135; 28 avril 2009, *K.H. e.a.* c. Slovaquie, §§ 60-69; grande chambre, 12 janvier 2010, *S. et Marper* c. Royaume-Uni, §§ 101-103, 119, 122 et 124; 18 avril 2013, *M.K.* c. France, §§ 37 et 42-44; 18 septembre 2014, *Brunet* c. France, §§ 35-37; 12 janvier 2016, *Szabó et Vissy* c. Hongrie, § 68; CJUE, grande chambre, 8 avril 2014, C-293/12, *Digital Rights Ireland Ltd*, et C-594/12, *Kärntner Landesregierung e.a.*, points 56-66).

B.15.1. 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, une portée analogue à celle de l'article 8 de la Convention européenne des droits de l'homme (CJUE, grande chambre, C-92/09 et C-93/09, 9 novembre 2010, *Volker und Markus Schecke GbR et autres*) 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.

B.15.2. La compatibilité de dispositions législatives avec les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, combinés avec des dispositions constitutionnelles analogues ou avec les articles 10 et 11 de la Constitution, ne peut être examinée par la Cour qu'en ce que les dispositions attaquées mettent en œuvre le droit de l'Union (CJUE, grande chambre, 26 février 2013, C-617/10, *Åklagaren*, points 17 et suivants).

En l'espèce, il convient de prendre en compte la directive 95/46/CE et le règlement général sur la protection des données.

B.15.3. Dès lors que les dispositions attaquées concernent le traitement de données à caractère personnel relevant de l'application de ces actes législatifs de l'Union européenne, les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne sont combinés

avec les dispositions constitutionnelles analogues ou avec les articles 10 et 11 de la Constitution.

Quant au moyen unique

B.16. Les griefs formulés par la partie requérante concernent principalement la compatibilité, avec le droit au respect de la vie privée, de divers aspects du système « push » et du « data mining » envisagé.

En ce qui concerne la prévisibilité de la loi

B.17. La partie requérante demande l'annulation des articles 2, 3 et 4 de la loi attaquée parce que l'ingérence dans le droit au respect de la vie privée ne serait pas compatible avec les dispositions mentionnées en B.9, en ce qu'il n'existerait pas de fondement ou de fondement légal suffisamment précis pour justifier l'ingérence visée par le législateur et en ce que les articles 3 et 4 ne seraient pas suffisamment précis.

B.18. Toute personne doit savoir de manière suffisamment précise les circonstances et conditions dans lesquelles une ingérence dans sa vie privée est autorisée, en particulier en ce qui concerne le traitement automatisé de données à caractère personnel. Toute personne doit dès lors avoir une idée suffisamment claire des données traitées, des personnes concernées par ce traitement de données et des conditions et finalités dudit traitement.

Eu égard aux articles 5, b), et 9, paragraphe 2, de la Convention n° 108 et au principe 3.4 de la Recommandation (2010)13, cette exigence s'applique d'autant plus lorsque les données à caractère personnel sont ensuite traitées par les services publics à d'autres fins que celles pour lesquelles elles ont initialement été obtenues.

B.19. Dans l'article 2, attaqué, le législateur a prévu que les sociétés de distribution et les gestionnaires de réseaux de distribution collectent et transmettent des données de consommation et des adresses obtenues à la Banque-carrefour de la sécurité sociale lorsque la consommation s'écarte du seuil de consommation moyenne correspondant à une composition

de ménage déterminée, que ces données sont filtrées par la BCSS, croisées avec d'autres données, dans le but de vérifier si l'intéressé est connu comme bénéficiaire de prestations sociales, et enfin que ces données sont transmises aux IPSS et aux inspecteurs sociaux, afin que ces derniers puissent contrôler, sur la base des données obtenues, combinées avec les données disponibles dans le réseau, telles qu'elles sont visées dans la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale (ci-après : la « loi sur la BCSS »), après autorisation du comité sectoriel de la sécurité sociale et de la santé, si des prestations sociales ont été octroyées sur la base d'une adresse fictive. Dans l'article 4, attaqué, le législateur a clairement prévu que les données de consommation ne peuvent être considérées que comme un élément complémentaire et non comme un élément déterminant pour conclure à une fraude de la part d'un bénéficiaire de prestations sociales.

Dans l'article 3, attaqué, le législateur a ouvert la possibilité, pour les IPSS, de procéder au regroupement des données pour effectuer des analyses de ces données qui doivent permettre à ces services de réaliser des contrôles plus ciblés, sur la base d'indicateurs de risque de fraude sociale au domicile.

L'article 104 de la loi-programme (I) du 29 mars 2012 prévoit en outre que les dispositions de la loi relative à la protection de la vie privée restent d'application, de sorte que les conditions générales de traitement de données à caractère personnel, qui sont visées à l'article 4 de cette loi, s'appliquent également dans le cadre de l'ingérence attaquée en l'espèce.

B.20. Compte tenu, en particulier, des travaux préparatoires mentionnés en B.4, il découle de ce qui précède que l'ingérence a un fondement légal, de sorte que toute personne peut connaître de manière suffisamment précise les circonstances et les conditions relatives au traitement de ses données à caractère personnel. L'ingérence dans le droit à la protection de la vie privée satisfait donc aux conditions mentionnées en B.13.2.

B.21. Néanmoins, la référence à l'article 101, faite aux paragraphes 2 et 3 de cet article, est manifestement une erreur matérielle, eu égard à la formulation de l'article 3 attaqué, et en particulier à la référence à des données « codées » ou « décodées », et compte tenu des travaux préparatoires mentionnés en B.7.2.2 et de la volonté, qui en découle, de s'inspirer des

règles de traitement des données à caractère personnel telles qu'elles sont appliquées par le SPF Finances.

A l'article 101/1, §§ 2 et 3, de la loi-programme (I) du 29 mars 2012, inséré par l'article 3, attaqué, les mots « dans le cadre de l'article 101, § 1 » et « visées à l'article 101, § 1er, » doivent être annulés.

En ce qui concerne le principe de légalité

Le délai de conservation des données

B.22. La partie requérante fait valoir qu'en ce qui concerne l'ingérence prévue par les articles 2 et 3 attaqués, le législateur n'a pas fixé toutes les conditions auxquelles il peut être porté atteinte au droit au respect de la vie privée, en ce que le délai précis de conservation des données serait fixé par le comité sectoriel de la sécurité sociale et de la santé.

B.23. L'article 4, § 1er, 4° et 5°, de la loi relative à la protection de la vie privée prévoit que les données à caractère personnel ne peuvent être conservées pour une durée excédant la durée nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues et que ces données doivent être, le cas échéant, rectifiées ou effacées. Compte tenu du fait que le législateur ne peut prévoir des règles distinctes et précises pour tous les cas spécifiques, il pouvait régler de manière générale les conditions de conservation des données à caractère personnel, ainsi que la durée de cette conservation.

Il découle de ce qui précède que le législateur a réglé les éléments essentiels de la durée de conservation des données.

Le grief formulé en B.22 n'est pas fondé.

En ce qui concerne le principe de proportionnalité

Le système « push »

B.24. La partie requérante demande l'annulation de l'article 2 attaqué parce que le système « push » qu'il contient irait au-delà de ce qui est nécessaire pour lutter contre la fraude sociale au domicile et parce que les garanties relatives aux délais de conservation, à l'intervention du comité sectoriel de la sécurité sociale et de la santé, aux droits de contrôle des intéressés, à la procédure et à la sécurité seraient inexistantes ou insuffisantes.

B.25. Eu égard au fait que le système « push » prévoit une ingérence importante dans la vie privée du fait de l'ampleur et de la technique du traitement de données à caractère personnel, cette ingérence doit non seulement avoir un fondement légal, mais aussi satisfaire aux conditions mentionnées en B.14.

B.26. Comme il a déjà été dit en B.2, le législateur visait à lutter de manière plus performante et plus efficace contre la fraude sociale, qui est étroitement liée à l'utilisation d'un domicile fictif.

Le législateur poursuivait donc un objectif légitime en adoptant la mesure attaquée.

B.27. Le législateur doit également poursuivre cet objectif en prenant une mesure adéquate.

B.28. Le législateur a pu raisonnablement estimer que le système « push » était adéquat pour atteindre l'objectif poursuivi, en ce qu'il permet, sans qu'il y ait *a priori* une présomption de fraude à charge d'un bénéficiaire spécifique, d'utiliser des données de consommation fondées sur une consommation anormale comme un signal autonome d'une éventuelle fraude au domicile, ce qui permet de mieux détecter l'usage d'adresses potentiellement fictives et d'exercer aussi ensuite des contrôles ciblés, même avec des capacités en personnel réduites.

B.29. En ce qui concerne la nécessité de l'ingérence dans le droit au respect de la vie privée lors du traitement de données à caractère personnel, il convient de déterminer quelle est

l'incidence de la réglementation attaquée sur cette vie privée, compte tenu des garanties existantes, et de vérifier si cette réglementation ne porte pas une atteinte disproportionnée aux garanties mentionnées en B.14.

B.30.1. Les autorités, services, organismes ou personnes qui sélectionnent, transmettent ou obtiennent ces données à caractère personnel par la méthode visée dans la loi attaquée sont tenus de respecter les dispositions applicables de la loi sur la protection de la vie privée.

B.30.2. En l'espèce, le législateur, par la loi relative à la protection de la vie privée, a choisi d'adopter un régime légal général, applicable à la fois au secteur public et au secteur privé (*Doc. parl.*, Chambre, 1990-1991, nr. 1610/1, p. 3), qui tienne néanmoins compte des particularités de certains secteurs et de la conciliation de toutes sortes d'intérêts. C'est pourquoi le législateur a expressément confirmé, dans l'article 104 de la loi-programme (I) du 29 mars 2012, l'application de la loi relative à la protection de la vie privée au système « push ».

B.30.3. La loi relative à la protection de la vie privée contient les règles qui sont essentielles à la protection du droit au respect de la vie privée : notamment des garanties individuelles (article 4) quant à l'enregistrement de données sensibles (articles 6 à 8); le droit d'accès et le droit de rectification (articles 10 et 12); la confidentialité et la sécurisation (article 16, § 4); la publicité des traitements et la large information des personnes concernées (articles 5 et 9); et le contrôle par un organe indépendant (article 31) et par les cours et tribunaux (article 14). Le responsable du traitement, désigné par le législateur, est donc soumis au respect de plusieurs obligations.

B.31. Néanmoins, l'importance, la nature et l'ampleur du traitement de données à caractère personnel instauré par le législateur requièrent des garanties spécifiques ou complémentaires.

Compte tenu du fait que le système attaqué consiste à signaler automatiquement - sans la moindre présomption préalable dans le chef des services publics à l'encontre de bénéficiaires individuels de prestations sociales - des soupçons de fraude au domicile, le législateur a choisi de soumettre les consommateurs de gaz, d'eau et d'électricité à un « profilage ». Cette technique a ceci de spécifique qu'elle se base sur le recours à certains paramètres pour repérer

comme signal un comportement déterminé (fraude), à travers des données de consommation relatives à un nombre indifférencié de personnes ou pour prévoir un tel comportement sur la base d'une analyse de cette masse de données. Ce signal résulte en l'espèce de la comparaison entre la consommation réelle d'eau, de gaz et d'électricité à une adresse déterminée et la consommation moyenne correspondant à la composition de ménage officiellement communiquée à cette même adresse.

Cette technique de traitement comporte néanmoins des risques en ce qui concerne le droit à la protection de la vie privée dont jouissent les intéressés (voir le rapport explicatif de la recommandation (2010)13, points 50-64), 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.

B.32.1. La partie requérante fait valoir que le législateur n'a pas désigné un responsable du traitement à chaque étape du système « push ».

B.32.2. Avant que le système « push » ne soit mis en application, le traitement des données de consommation et des adresses dans le cadre de l'exécution normale par les sociétés de distribution et par les gestionnaires de réseaux de distribution se fait conformément aux dispositions de la loi relative à la protection de la vie privée, ces sociétés et ces gestionnaires étant tenus de désigner pour ce faire un responsable au sens de l'article 1er, § 4, de la loi relative à la protection de la vie privée.

En ce qui concerne la sélection des données à transmettre et le flux de données à proprement parler dans le système attaqué, le législateur a cependant choisi de désigner la Banque-carrefour de la sécurité sociale comme responsable du traitement des données.

Le législateur a dès lors prévu que le respect des obligations mentionnées en B.30 dans le cadre du système « push » incombe d'abord à la Banque-carrefour de la sécurité sociale, qui est aussi responsable du respect de ces obligations par le sous-traitant, au sens de l'article 1er, § 5, de la loi relative à la protection de la vie privée, en l'occurrence les sociétés de distribution et les gestionnaires de réseaux de distribution.

Le grief formulé en B.32.1 n'est pas fondé.

B.33.1. La partie requérante fait valoir que le traitement des données à caractère personnel, tel qu'il est prévu dans le système attaqué, n'est pas minimal.

B.33.2. Dans le système attaqué, le législateur oblige les sociétés de distribution et les gestionnaires de réseaux de distribution à collecter les seules données de consommation et les adresses liées à ces données. L'obligation ainsi imposée est limitée à deux types de données qui sont utilisées pour l'exploitation normale.

Les sociétés de distribution et les gestionnaires de réseaux de distribution sont dès lors tenus de transmettre les données de consommation et les adresses à la Banque-carrefour de la sécurité sociale. Le législateur a toutefois fixé un seuil d'écart pour la transmission de ces données, en l'occurrence un écart de plus de 80 % par rapport à la consommation moyenne correspondant à la composition de ménage officiellement communiquée.

B.33.3. Il peut être admis qu'il existe un lien entre la composition du ménage et la consommation d'eau, de gaz et d'électricité. Il peut dès lors être déduit, sur la base des données de consommation, un écart par rapport à la consommation moyenne probable pour le type de ménage officiellement communiqué. Compte tenu de ce qui est dit en B.3.5 et de la marge d'appréciation dont dispose le législateur confronté à des évaluations complexes, il n'apparaît pas que le seuil précité soit manifestement déraisonnable.

B.34. Ce seuil permet en effet de limiter le nombre de personnes dont les données doivent être transmises à la Banque-carrefour de la sécurité sociale au nombre de personnes pour lesquelles il existe des motifs raisonnables qui justifient la poursuite de l'enquête, d'autant plus qu'il s'agit d'un écart significatif.

B.35. Avant de transmettre les données obtenues aux inspecteurs sociaux ou aux IPSS, la Banque-carrefour de la sécurité sociale vérifie, au moyen du répertoire des personnes (article 6 de la loi sur la Banque-carrefour de la sécurité sociale), après croisement avec les données du Registre national, si les données de consommation et les adresses obtenues concernent un bénéficiaire de prestations sociales, de sorte que, lors de la dernière étape, ne sont finalement transmises que les données relatives aux bénéficiaires à l'égard desquels il existe une présomption de fraude sociale au domicile.

B.36. Il découle de ce qui précède que le législateur a prévu de filtrer ce flux de données structurel et volumineux et de le limiter à ce qui est nécessaire pour lutter contre la fraude sociale au domicile.

Dans le système « push », les services publics ont donc seulement accès aux données dont ils ont besoin pour contrôler le caractère fictif ou non du domicile d'un bénéficiaire de prestations sociales. Ce traitement n'a dès lors pas d'effets disproportionnés.

Le grief formulé en B.33.1 n'est pas fondé.

B.37.1. La partie requérante fait valoir que le traitement des données personnelles des intéressés viole leurs droits de contrôle, en ce que l'exercice direct de ces droits est exclu.

B.37.2. L'article 3, § 5, 3°, de la loi relative à la protection de la vie privée prévoit que les articles 9, 10, § 1er, et 12 de la même loi (droit à l'information, droit d'accès, droit de rectification et droit d'effacement) ne s'appliquent pas aux autorités publiques désignées par arrêté royal en vue de l'exercice de leurs missions de police administrative. En exécution de l'article 3, § 5, 3°, de la loi relative à la protection de la vie privée, l'article 1er de l'arrêté royal du 11 mars 2015 dispose :

« § 1. Les articles 9, 10, § 1er, et 12 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 ne sont pas applicables aux inspecteurs sociaux et aux fonctionnaires des autorités publiques énumérées au § 2, dans le cadre de leurs missions de police administrative visées dans Livre 1er, Titre 2 et Titre 4, Chapitre 3 du Code pénal social.

§ 2. Ces autorités sont :

- Service public fédéral Emploi, Travail et Concertation sociale;
- Office national de l'Emploi;
- Office national de Sécurité sociale;
- Office national des Vacances Annuelles;
- Institut national d'Assurance Maladie-Invalidité;
- Agence fédérale pour les allocations familiales;

- Office des régimes particuliers de sécurité sociale;
- Fonds des Accidents du Travail;
- Fonds des Maladies professionnelles;
- Office de contrôle des Mutualités et des Unions nationales de mutualités;
- Office national des Pensions;
- Institut national des assurances sociales pour travailleurs indépendants ».

L'intéressé ne peut donc exercer directement ses droits de contrôle sur le traitement de données par les inspecteurs sociaux et par les IPSS, dans la mesure où ce traitement relève de l'exécution de leurs missions de police administrative.

B.37.3. L'article 13 de la loi relative à la protection de la vie privée dispose toutefois :

« Toute personne justifiant de son identité a le droit de s'adresser sans frais à la Commission de la protection de la vie privée pour exercer les droits visés aux articles 10 et 12 à l'égard des traitements de données à caractère personnel visés à l'article 3, §§ 4, 5, 6 et 7.

Le Roi détermine, après avis de la Commission de la protection de la vie privée et par arrêté délibéré en Conseil des ministres, les modalités d'exercice de ces droits.

La Commission de la protection de la vie privée communique uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires.

Toutefois, le Roi détermine, après avis de la commission de la protection de la vie privée, par arrêté délibéré en Conseil des ministres, quelle information peut être communiquée à l'intéressé lorsque la demande de celui-ci porte sur un traitement de données à caractère personnel géré par des services de police en vue de contrôles d'identité ».

L'intéressé peut dès lors exercer ses droits de contrôle en s'adressant à la Commission de la protection de la vie privée.

B.38.1. En vertu de l'article 9, paragraphe 2, de la Convention n° 108, il est possible de déroger au droit de contrôle visé à l'article 8 de cette Convention, dans la mesure où une loi le prévoit et lorsque cette dérogation constitue, dans une société démocratique, une mesure nécessaire à la protection de la sécurité de l'Etat, à la sûreté publique, aux intérêts monétaires

de l'Etat, à la répression des infractions pénales et à la protection de la personne concernée et des droits et libertés d'autrui.

B.38.2. L'effectivité et l'efficacité de la lutte contre la fraude - et donc de la protection des intérêts financiers de l'Etat et des droits d'autrui dans un système social - peuvent justifier la limitation des droits de contrôle des intéressés sur le traitement de leurs données personnelles, pour autant que cette limitation du droit d'accès en ce qui concerne les missions de police administrative porte uniquement sur les données relatives à des bénéficiaires de prestations sociales et que la durée de l'exclusion du droit d'accès direct n'excède pas les besoins de l'enquête.

Il découle de ce qui est dit en B.37 que la non-application des articles 9, 10 et 12 de la loi relative à la protection de la vie privée et le droit d'accès indirect, prévu par l'article 13 de la loi relative à la protection de la vie privée, sont limités aux données qui sont traitées par les douze instances visées et par les inspecteurs sociaux, dans le cadre de leurs missions de police administrative. En ce qui concerne les données qui sont traitées par ces institutions publiques et par ces inspecteurs sociaux, pour d'autres missions et à d'autres fins, ces derniers sont tenus au respect des articles 9, 10 et 12 de la loi relative à la protection de la vie privée.

Toutefois, lorsque les besoins d'une enquête ne le justifient plus, il n'est pas raisonnablement justifié de refuser à l'intéressé l'accès direct à ses données personnelles et le contrôle de ces dernières.

B.38.3. Sous réserve de ce qui est mentionné en B.38.2, dernier alinéa, le grief formulé en B.37.1 n'est pas fondé.

B.39.1. La partie requérante fait valoir l'absence de garanties suffisantes en termes de sécurité et de confidentialité.

B.39.2. L'article 16, § 4, de la loi relative à la protection de la vie privée prévoit que le responsable du traitement ainsi que le sous-traitant lui-même doivent prendre les mesures organisationnelles et techniques requises pour protéger les données à caractère personnel, compte tenu de l'état de la technique en la matière, de la nature des données à protéger et des risques potentiels. Le législateur a explicitement désigné les risques à prendre en compte lors

de la mise en œuvre de ces mesures de sécurité (destruction accidentelle de données, perte accidentelle de données, modification non autorisée des données, etc.).

B.39.3. Outre les garanties contenues dans la loi relative à la protection de la vie privée, le législateur a également prévu, dans la loi relative à la Banque-carrefour de la sécurité sociale, des garanties concernant le secret professionnel, la désignation d'un conseiller en sécurité et les mesures de sécurité (articles 22, 23, 24, 25 et 28 de la loi sur la Banque-carrefour de la sécurité sociale). En ce qui concerne l'inspection sociale également, l'article 58 du Code pénal social garantit la confidentialité des données sociales mises à disposition des inspecteurs sociaux. Aux articles 213 à 215 du Code pénal social, le législateur a également prévu des sanctions en cas de non-respect de la confidentialité des données ou en cas d'absence des mesures de sécurité requises.

B.39.4. Il ressort de ce qui précède que le législateur a prévu des garanties pour assurer la sécurité et la confidentialité des données à caractère personnel qui sont traitées.

Le grief formulé en B.39.1 n'est pas fondé.

B.40. La partie requérante invoque l'absence de garanties procédurales, telles qu'elles sont par exemple contenues 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.

B.41. Les données traitées selon le système « push » peuvent uniquement être utilisées par les services publics comme indication supplémentaire en vue de déterminer si un bénéficiaire de prestations sociales a commis une fraude au domicile (article 102 de la loi-programme (I) du 29 mars 2012, tel qu'il a été remplacé par l'article 4 de la loi attaquée), ce qui exclut tout effet défavorable immédiat pour l'intéressé. En effet, les instances publiques compétentes doivent, le cas échéant, disposer d'autres éléments pour prendre une décision défavorable (par exemple des sanctions en cas de fraude) à l'encontre d'un bénéficiaire de prestations sociales. Dans l'article 103 de la loi-programme (I) du 29 mars 2012, tel qu'il a été modifié par l'article 5 de la loi attaquée, le législateur a prévu que les inspecteurs sociaux informent le bénéficiaire ou, le cas échéant, un tiers, du fait qu'ils peuvent utiliser des données de consommation le concernant, pour les besoins de l'enquête administrative. En

vertu de l'article 79 du Code pénal social, les intéressés ont également accès au dossier administratif.

B.42. Si, finalement, l'enquête donne lieu à un « constat » de fraude au domicile repérée au moyen du système « push », le bénéficiaire de prestations sociales concerné peut en outre démontrer en fait ou en droit qu'il n'y a pas eu fraude au domicile. En vertu des principes généraux de bonne administration ou des règles relatives à la procédure pénale, l'intéressé bénéficie de garanties en ce qui concerne ses droits de défense.

B.43. L'article 14 de la loi relative à la protection de la vie privée prévoit que le président du tribunal de première instance, siégeant comme en référé, connaît de toute demande relative au droit accordé par ou en vertu de la loi, d'obtenir communication de données à caractère personnel, et de toute demande tendant à faire rectifier, supprimer ou interdire d'utiliser toute donnée à caractère personnel inexacte ou, compte tenu du but du traitement, incomplète ou non pertinente, dont l'enregistrement, la communication ou la conservation sont interdits, au traitement de laquelle la personne concernée s'est opposée ou encore qui a été conservée au-delà de la période autorisée. En vertu de l'article 32, § 3, de la loi relative à la protection de la vie privée, le président de la Commission de la protection de la vie privée peut, le cas échéant après une plainte de l'intéressé, soumettre au tribunal de première instance tout litige concernant l'application de cette loi et de ses mesures d'exécution.

L'intéressé dispose dès lors de voies de recours pour soumettre au contrôle du juge l'ingérence dans son droit au respect de la vie privée résultant du traitement de ses données personnelles.

B.44. Il ressort de ce qui précède que la loi attaquée offre des garanties procédurales suffisantes.

Le grief formulé en B.40 n'est pas fondé.

B.45. La partie requérante fait valoir que le législateur n'a pas fixé de délais de conservation suffisamment spécifiques.

B.46. En vertu de l'article 4, § 1er, 3°, 4° et 5°, de la loi relative à la protection de la vie privée, eu égard à l'objectif spécifique poursuivi, l'obligation s'applique, lors de chaque phase, de ne plus traiter les données à caractère personnel qui ne sont pas (ou qui ne sont plus) pertinentes ou qui sont erronées, de les rectifier ou de les supprimer, et en tout cas de ne pas les conserver plus longtemps que nécessaire pour atteindre l'objectif poursuivi, en l'occurrence la collecte et la transmission de données de consommation à la BCSS, le recoupement et le transfert de ces données par la BCSS aux services publics intéressés. Les IPSS et les inspecteurs sociaux sont également soumis à l'interdiction de conserver les données au-delà de la période nécessaire pour contrôler l'utilisation d'une adresse fictive à des fins de fraude aux allocations, de sorte qu'en tout état de cause, ces données ne peuvent être conservées au-delà du délai de prescription prévu en cas de fraude.

Le grief formulé en B.45 n'est pas fondé.

B.47. La partie requérante fait encore valoir que le législateur n'a pas choisi la mesure la moins extrême pour renforcer la lutte contre la fraude sociale au domicile.

B.48. Il ressort des travaux préparatoires mentionnés en B.2 que, pour lutter contre la fraude sociale au domicile, le législateur a envisagé deux façons d'utiliser les données de consommation : le système « pull » (*statu quo*) et le système « push » (nouvel instrument).

B.49. Dans les deux systèmes, en cas de suspicion de fraude, les services publics reçoivent uniquement, en vue du contrôle de la fraude sociale au domicile, les données de consommation de bénéficiaires de prestations sociales.

La différence essentielle entre les deux systèmes porte sur la façon dont l'autorité publique arrive à la présomption de fraude précitée. Dans le système attaqué, la présomption est alimentée par des procédés techniques permettant une analyse automatique et structurelle des données de consommation de tous les consommateurs en vue de déclencher des signaux d'alerte sur la base d'un profil, alors que le système « pull » n'utilise aucune donnée concernant des tiers.

B.50. Eu égard au fait que la lutte contre la fraude sociale au domicile est une lutte permanente nécessitant des efforts continus, et que la fraude et la lutte contre celle-ci sont sujettes à des changements de comportement social, notamment eu égard aux moyens techniques disponibles, le législateur a pu raisonnablement estimer que le système « push » permet de lutter de manière plus effective et efficace contre la fraude sociale.

B.51. De l'explication du système « pull » donnée en B.1.3, il ressort que ce système requiert un investissement énorme en personnel et en moyens pour permettre de lutter efficacement contre la fraude sociale au domicile. Eu égard au rayon d'action limité de ce système, ce dernier ne semble pas permettre de soumettre le même nombre de bénéficiaires sociaux à une enquête et ne permet donc pas non plus de détecter le même nombre de cas présumés de fraude que le système « push » attaqué. Ceci vaut également *mutatis mutandis* pour les instruments de recherche évoqués par la partie requérante, tels que la visite domiciliaire, la collecte d'informations et l'audition de personnes (articles 24, 26 et 27 du Code pénal social). En ce qui concerne la réclamation spécifique et individualisée de données, le système « pull » est également de nature à stigmatiser les intéressés - d'une part, en tant que bénéficiaires de prestations sociales et, d'autre part, en tant que fraudeurs présumés - et donc à avoir des conséquences néfastes sur la vie privée.

B.52. Du fait du rôle de la BCSS, le système « push » empêche les sociétés de distribution et les gestionnaires de réseaux de distribution de connaître, parmi leurs consommateurs, ceux qui bénéficient de prestations sociales, ce qui réduit au strict nécessaire l'ingérence dans la vie privée des bénéficiaires de prestations sociales. Il ressort également de ce qui est dit en B.29 à B.44 que le législateur a prévu les conditions et garanties matérielles et procédurales nécessaires en termes d'ingérence dans la vie privée.

B.53. Il ressort de ce qui précède, et en particulier compte tenu de ce qui est mentionné en B.1.2 et B.52 et des différences entre les deux systèmes, que le législateur pouvait raisonnablement considérer que le système « push », tel qu'il est instauré par l'article 2 de la loi attaquée, ne va pas au-delà de ce qui est nécessaire pour détecter, décourager et combattre la fraude sociale au domicile de manière performante et efficace.

Le grief mentionné en B.47 n'est pas fondé.

B.54. La Cour doit encore vérifier si le système « push » attaqué, qui, tel qu'il est exposé en B.3, implique le « profilage » et la technique de traitement « data mining », n'engendre pas des effets disproportionnés.

B.55. Eu égard à l'objectif poursuivi, qui consiste notamment à détecter des cas présumés de fraude au domicile jusque-là impossibles ou très difficiles à détecter, et compte tenu du caractère dissuasif du système « push », des changements dans le comportement de personnes du groupe-cible, et de l'imprévisibilité des agissements frauduleux et du nombre de cas, il n'est pas sans justification raisonnable qu'en fixant la mesure, le législateur ne puisse faire aucune estimation globale et définitive des recettes et coûts liés au système et donc à l'efficacité de celui-ci.

Le grief mentionné en B.54 n'est pas fondé.

Le « datawarehouse » et le « data mining »

B.56. La partie requérante demande l'annulation de l'article 3 parce que le regroupement et l'analyse de données disponibles par les IPSS iraient au-delà de ce qui est nécessaire pour lutter contre la fraude sociale au domicile et parce que les garanties telles que la condition d'une autorisation décernée par le comité sectoriel de la sécurité sociale et de la santé et les conditions d'intégrité et de confidentialité seraient inexistantes ou insuffisantes.

B.57. Le regroupement des données dont peuvent disposer les IPSS et les inspecteurs sociaux qui en relèvent le cas échéant, ainsi que la recherche, dans ces données, d'éventuels corrélations et indicateurs concernant le risque d'utilisation d'une adresse fictive peuvent raisonnablement être considérés comme un moyen approprié pour renforcer la lutte contre la fraude sociale au domicile.

B.58. Ainsi qu'il ressort de ce qui a été mentionné en B.30, les garanties offertes par la loi relative à la protection de la vie privée s'appliquent également au traitement qui découle de l'article 3 attaqué.

B.59. La partie requérante fait valoir que l'article 3 attaqué ne requiert aucune autorisation de la part d'un comité sectoriel de la sécurité sociale et de la santé, en ce qui concerne la transmission de données aux inspecteurs sociaux.

B.60. Compte tenu de l'annulation mentionnée en B.21 et de la portée, limitée aux IPSS, de l'article attaqué, le grief formulé en B.59 n'est pas fondé.

B.61. Enfin, la partie requérante fait valoir que l'article 3 attaqué viole les principes d'intégrité et de confidentialité, en ce qu'il ne prévoit pas de garanties suffisantes.

B.62. L'article 16, § 4, de la loi relative à la protection de la vie privée impose aux IPSS, en leur qualité de responsables du traitement des données, de prendre des mesures organisationnelles et techniques adéquates, qui sont nécessaires pour garantir la protection des données à caractère personnel, compte tenu de l'état de la technique et de la nature des données à protéger, ainsi que des risques potentiels. A cet égard, le législateur a explicitement désigné les risques à prendre en compte lors de la mise en œuvre de ces mesures de sécurité (destruction accidentelle de données, perte accidentelle de données, modification non autorisée des données, etc.).

Le grief mentionné en B.61 n'est pas fondé.

B.63. Il ressort de ce qui précède, compte tenu également du caractère initialement codé des analyses visées, que l'article 3 de la loi attaquée ne va pas au-delà de ce qui est nécessaire pour renforcer la lutte contre la fraude sociale au domicile. La détection de corrélations et de nouveaux indices est en outre nécessaire pour suivre les évolutions des actes frauduleux et traquer d'éventuels cas de fraude.

Les griefs mentionnés en B.56 ne sont pas fondés.

Par ces motifs,

la Cour

- annule les mots « dans le cadre de l'article 101, § 1er, » et « visées à l'article 101, § 1er », contenus respectivement dans les paragraphes 2 et 3 de l'article 101/1 de la loi-programme (I) du 29 mars 2012, tels qu'ils ont été insérés par l'article 3 de la loi du 13 mai 2016 « modifiant la loi-programme (I) du 29 mars 2012 concernant le contrôle de l'abus d'adresses fictives par les bénéficiaires de prestations sociales, en vue d'introduire la transmission systématique de certaines données de consommation de sociétés de distribution et de gestionnaire de réseaux de distribution vers la BCSS améliorant le datamining et le datamatching dans la lutte contre la fraude sociale »;

- rejette le recours pour le surplus, sous réserve de ce qui est dit en B.38.2, dernier alinéa.

Ainsi rendu en langue néerlandaise, en langue française et en langue allemande, conformément à l'article 65 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, le 15 mars 2018.

Le greffier, Le président,

P.-Y. Dutilleux E. De Groot