DOCTRINE

La loi du 30 juillet 2018 : l'échange de données à caractère personnel au sein du secteur public

Manon Knockaert[1]

Suite à l'entrée en vigueur du Règlement général sur la protection des données (« RGPD »), le législateur belge a adapté la législation. Désormais, les échanges de données entre les organismes du secteur public et entre les organismes publics et le secteur privé doivent être encadrés par un protocole. Le présent commentaire est l'occasion d'analyser en profondeur le contenu du protocole et son fonctionnement, tout en prêtant attention aux avis – appelant à la plus grande vigilance – émis par le Conseil d'État et l'ancienne Commission de protection de la vie privée (« CPVP »).

• • •

Following the entry into force of the General Data Protection Regulation ("GDPR"), the Belgian legislator adapted its national legislation. Now, the exchange of personal data between public sector bodies and between public and private sector bodies must be governed by a protocol. This commentary proposes an in-depth analysis of the content of the protocol and its functioning, while paying attention to the opinions – which call upon the greatest vigilance – issued by the Conseil d'État and the former Commission de Protection de la Vie Privée ("CPVP").

I. INTRODUCTION

Le Règlement général sur la protection des données (« RGPD »)[2] a mis un véritable coup de projecteur sur la problématique de la vie privée des individus et du traitement de leurs informations à caractère personnel : coup de lumière nécessaire suite à l'utilisation croissante des nouvelles technologies, collectant et traitant un nombre de plus en plus important de données à caractère personnel.

Ce nouveau texte laissant une marge de manœuvre aux États membres, le législateur fédéral belge a adopté la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel[3]. L'avant-projet de loi a

[1] Chercheuse au CRIDS-NaDI UNamur.

[2] 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, *J.O.*, L 119, 4 mai 2016, p. 1 (ci-après « RGPD »).

[3] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, p. 68616 (ci-après « la loi du 30 juillet 2018 »).

été soumis à l'avis de l'ancienne Commission de la protection de la vie privée (« CPVP »), devenue désormais Autorité de protection des données (« APD ») et à l'avis de la section de législation du Conseil d'État (« SLCE ») rendus respectivement le 11 avril[4] et le 19 avril 2018[5]. Il a fallu attendre le 11 juin 2018 pour connaître le premier projet de loi belge en la matière[6] suivi par un second avis de l'ancienne CPVP[7].

Composée de 286 dispositions, la loi belge du 30 juillet 2018 est divisée en six titres principaux. Le premier est générique et porte sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Le second concerne les traitements opérés par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales. En troisième lieu, vient une catégorie résiduaire pour les traitements réalisés par des autorités autres que celles visées aux deux titres précédents. Loin d'être anecdotique, le quatrième titre organise les traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques. Les deux derniers titres ont trait aux voies de recours et aux sanctions.

L'objet de cette contribution est de présenter le cadre juridique belge entourant l'échange de données à caractère personnel entre autorités publiques. La première partie de cette contribution permet une contextualisation de la matière en exposant le fonctionnement de l'administration belge, fonctionnement bouleversé par l'arrivée d'outils numériques. La deuxième partie est consacrée à la loi du 30 juillet 2018 et à sa section réservée au secteur public. À cet égard, nous nous concentrons principalement sur le titre premier, réservant une section spécifique au secteur public aux articles 19 à 23 et prévoyant certaines particularités. Nous attirons toutefois l'attention du lecteur sur le fait que les articles portant sur les principes du traitement, les limitations aux droits de la personne concernée ainsi que sur les obligations du responsable du traitement et du sous-traitant restent d'application. Une attention particulière est accordée à la mise en place d'un protocole encadrant le transfert des données à caractère personnel.

II. LE SECTEUR PUBLIC DANS LA LOI DU 30 JUILLET 2018

A. L'administration belge

Afin de mener à bien leurs missions de service public, les organismes du secteur public recueillent et disposent d'innombrables informations, pouvant par ailleurs constituer des données à caractère personnel[8]. Force est de

4 CPVP, avis n° 33/2018 concernant l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, 11 avril 2018.

5 Avis de la section de législation du Conseil d'État précédent la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, p. 68616.

6 Projet de loi du 11 juin 2018 relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *Doc. parl.*, Ch. repr., 2017-2018, n° 54-3126/001.

7 Avis n° 52/2018 concernant l'analyse du suivi de l'avis n° 33/2018 du 11 avril 2018 de la Commission de la protection de la vie privée et du projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel déposé à la Chambre des représentants le 11 juin 2018 (CO-A-2018-049), 22 juin 2018.

8 Selon l'article 4.1 du RGPD, une donnée à caractère personnel est définie comme « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un

constater que, face à l'explosion du numérique, les organismes publics ont dû revoir leur méthode de fonctionnement. Les charges administratives et le fonctionnement cloisonné font désormais place à une architecture en réseaux reposant sur le principe de la collecte unique des données à caractère personnel[9].

Ce principe poursuit deux objectifs.

Premièrement, il évite à chaque administration de collecter et de traiter individuellement les données à caractère personnel des citoyens.

Deuxièmement, le fonctionnement en réseaux permet d'alléger la charge administrative reposant sur le citoyen qui ne doit ainsi communiquer qu'une seule fois ses informations personnelles à une autorité publique. Dès lors, les mêmes informations ne peuvent plus être demandées plusieurs fois au citoyen, à charge pour l'organisme public ayant besoin d'une information d'en adresser la demande à l'autorité publique détenant déjà les données à caractère personnel.

En vue de faciliter la communication entre les différentes autorités publiques et le flux de circulation des données à caractère personnel, la Belgique recourt à la mise en place de sources authentiques de données. L'organisme public qui se voit légalement attribuer la qualité de source authentique de données est alors chargé de collecter et de conserver certaines données à caractère personnel des citoyens et d'être garant de leur qualité[10].

En parallèle, la Belgique met en place des « intégrateurs de services »[11]. Plaque tournante du réseau et point de contact pour les organismes publics, cette infrastructure est chargée d'assurer la circulation des données à caractère personnel provenant de sources authentiques[12]. Le principe de la collecte unique se matérialise également dans la création d'une banque de données issues de sources authentiques. Cette dernière est en réalité une source authentique enrichie de données provenant d'autres sources authentiques afin de fournir une information plus complète[13].

Dans son avis portant sur la loi du 30 juillet 2018, la SLCE n'a pas manqué de souligner l'existence de nombreux transferts de données à caractère personnel entre autorités publiques en Belgique. Eu égard à la fréquence des ingérences dans le droit au respect de la vie privée générées par ce contexte organisationnel, le

numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

9 E. Degrave, « L'administration belge organisée en réseaux : réutilisation des données à caractère personnel et protection de la vie privée », *Données urbaines et smart cities*, J.-B. Aubry et V. De Gregorio, dir., Berger-Levrault, 2017, pp. 184-187. Voy. également E. Degrave, *L'e-Gouvernement et la protection de la vie privée : Légalité, transparence et contrôle,* Bruxelles, Larcier, 2014.

10 Sur ce sujet, voy. E. Degrave, « L'administration belge organisée en réseaux : réutilisation des données à caractère personnel et protection de la vie privée », *op. cit.*, pp. 183-196. Voy. également E. Degrave, « L'intégrateur de services fédéral au cœur de la simplification administrative », *A.P.T.*, 4, pp. 518-536 ; C. de Terwangne, E. Degrave, A. Delforge et L. Gérard, *La protection des données à caractère personnel en Belgique : manuel de base*, 2019, Bruxelles, Politeia, p. 164.

11 Loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de service fédéral, *M.B.*, 29 août 2012, p. 53170.

12 Pour plus d'informations, voy. E. Degrave, « L'administration belge organisée en réseaux : réutilisation des données à caractère personnel et protection de la vie privée », *op. cit.*, pp. 183-196. Voy. également E. Degrave, « L'intégrateur de services fédéral au cœur de la simplification administrative », *op. cit.*

13 C. Fievet, L. Gérard, N. Gillard, M. Knockaert, A. Michel, J. Mont, K. Rosier, T. Tombal et O. Vanreck, « Droit au respect de la vie privée et à la protection des données en lien avec les technologies de l'information », in *Chronique de jurisprudence en droit des technologies de l'information : 2015-2017*, H. Jacquemin et T. Tombal (coord.), *R.D.T.I.*, 2017, nos 68-69, p. 152.

Conseil d'État insiste sur l'importance de la mise en place d'un cadre législatif consciencieux pour les échanges de données à caractère personnel en insistant sur le fait que le droit à la protection de la vie privée consacré aux articles 8 de la Convention européenne des droits de l'homme et 22 de la Constitution « n'est cependant pas absolu. Il n'exclut pas toute ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée, mais il est requis qu'elle soit prévue par une disposition législative suffisamment précise, qu'elle réponde à un besoin social impérieux dans une société démocratique et qu'elle soit proportionnée à l'objectif légitime qu'elle poursuit. Ces dispositions engendrent de surcroît l'obligation positive, pour l'autorité publique, de prendre des mesures qui assurent le respect effectif de la vie privée, même dans la sphère des relations entre les individus »[14]. Le Conseil d'État poursuit en insistant sur le fait qu'« un transfert de données d'une autorité publique à une autre constitue une ingérence dans le droit à la protection de la vie privée des personnes concernées. En vertu de l'article 8 de la Convention européenne des droits de l'homme et de l'article 22 de la Constitution, tel qu'interprété par une jurisprudence constante de la Cour constitutionnelle, pareille ingérence doit notamment reposer sur une base légale, être proportionnée par rapport à l'objectif poursuivi et être organisée de manière suffisamment précise pour être prévisible pour le citoyen »[15].

B. Le secteur public et l'échange de données à caractère personnel par la loi du 30 juillet 2018 : le protocole

Apport original de la loi du 30 juillet 2018, les autorités publiques fédérales se voient consacrer un espace réservé dans le chapitre relatif au responsable du traitement et au sous-traitant. En effet, l'article 20, § 1er dispose que : « Sauf autre disposition dans des lois particulières, en exécution de l'article 6.2 du règlement, l'autorité publique fédérale qui transfère des données à caractère personnel sur la base de l'article 6.1 c) et e), du règlement à tout autre autorité publique ou organisation privée, formalise cette transmission pour chaque type de traitement par un protocole entre le responsable du traitement initial et le responsable du traitement destinataire des données ».

En conséquence, lorsque le transfert des données à caractère personnel par une autorité publique fédérale est fondé sur la nécessité du respect d'une obligation légale à laquelle le responsable du traitement est soumis[16] ou lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique[17], ce transfert – qu'il ait pour destination un autre organisme du secteur public ou privé – doit être formalisé dans un protocole obligatoire. L'ancienne CPVP, dans son avis portant sur l'avant-projet de loi, avait insisté sur le fait que le protocole ne pourrait en aucun cas suppléer au cadre légal entourant le traitement et la circulation des informations par les sources authentiques de données à caractère personnel, le protocole ne devant concerner que les modalités pratiques[18].

14 Avis précédent la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, p. 68616, p. 5.

15 Avis de la section de législation du Conseil d'État précédent la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, p. 68616, p. 21.

16 Article 6.1 c), du RGPD.

17 Article 6.1 e), du RGPD.

18 CPVP, avis n° 33/2018 concernant l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, 11 avril 2018, p. 33, § 154.

1. Objectifs de l'instauration d'un protocole

Dans l'Exposé des motifs, le législateur souligne les deux objectifs principaux poursuivis par la mise en place d'un protocole[19].

Premièrement, le protocole facilite les transferts de données à caractère personnel au départ des autorités publiques fédérales[20].

Deuxièmement, la démarche s'inscrit dans la continuité de celle entamée par le législateur européen de responsabilisation de tous les intervenants dans la chaîne du traitement des données à caractère personnel. En effet, suite à la suppression du mécanisme de déclaration préalable des traitements à la CPVP par le RGPD et à la suppression des comités sectoriels chargés d'autoriser ou de refuser les transferts de données entre certains organismes publics par la loi du 3 décembre 2017[21], le protocole a vocation à obliger les responsables du traitement à être vigilants lors d'un transfert de données à caractère personnel et à vérifier sa légalité, à l'instar de l'obligation de tenue d'un registre des activités de traitement[22] et de la réalisation d'une éventuelle analyse d'impact. De surcroît, le responsable du traitement n'est pas seulement tenu au respect des obligations légales européennes et nationales pour le traitement de données, mais il doit également être en mesure de le démontrer[23]. La réalisation d'un protocole complet et précis permettra dès lors au responsable du traitement de garantir l'accomplissement de ces deux obligations.

2. Champ d'application

Le RGPD laissant le soin à chaque État membre de définir la notion d'« autorité publique », l'article 5 de la loi belge précise qu'il s'agit de : « (1°) L'État fédéral, les entités fédérées et les autorités locales ; (2°) les personnes morales de droit public qui dépendent de l'État fédéral, des entités fédérées ou des autorités locales et enfin (3°) les personnes, quelles que soient leur forme et leur nature qui ont été créées pour satisfaire spécifiquement des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial, […] dotées de la personnalité juridique et dont soit l'activité est financée majoritairement par les autorités publiques ou organismes mentionnés au 1° ou 2°, soit plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance […] désignés par ces autorités ou organismes »[24].

Ces autorités publiques doivent donc, lors de chaque transfert de données vers un autre

19 Voy. projet de loi du 11 juin 2018 relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, Exposé des motifs, *Doc. parl.*, Ch. repr., 2017-2018, n° 54-3126/001, p. 44.

20 Projet de loi du 11 juin 2018 relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, Exposé des motifs, *Doc. parl.*, Ch. repr., 2017-2018, n° 54-3126/001, p. 44.

21 Article 109 de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018, p. 989. Avant leur suppression, les Comités sectoriels étaient au nombre de cinq : le comité sectoriel de la Banque-Carrefour des entreprises, le comité sectoriel du Registre national, le comité de surveillance statistique, le comité sectoriel de la Sécurité sociale et de la Santé, ainsi que le comité sectoriel pour l'Autorité fédérale. Si le législateur belge ne justifie pas une telle suppression par la mise en application du principe de responsabilisation, nul doute qu'il en est le résultat. Sur le sujet, voy. également L. Gerard, « Le Comité de sécurité de l'information : illustration d'une incohérence législative », *R.D.T.I.*, 2018, p. 55.

22 À cet égard, la loi du 30 juillet 2018 prévoit et organise la tenue d'un registre des activités de traitement en son article 55.

23 E. Degrave, « Le règlement général sur la protection des données et le secteur public », *Rev. dr. commun.*, 2018, p. 5. Voy. également C. de Terwangne, K. Rosier et B. Losdyck, « Le règlement européen relatif à la protection des données à caractère personnel : quelles nouveautés ? », *J.D.E.*, 2017.

24 Par exemples, l'État, les régions, les communes et les services publics sont considérés comme des autorités publiques.

organisme public ou une entité privée, mettre en place ce protocole. Nous verrons que son contenu fait sensiblement écho aux principes du traitement prévus dans le RGPD, témoignant ainsi de l'objectif d'amener le responsable du traitement à se poser les bonnes questions. L'ancienne Commission de protection de la vie privée y voit une étape clé dans l'instauration d'une routine autour de la question du traitement des données au caractère personnel au sein du secteur public[25].

3. Contenu

Si l'établissement d'un protocole est obligatoire et ne souffre d'aucune exception, remarquons que son contenu est facultatif par l'emploi du terme « pouvoir ». Ce vocabulaire n'a échappé ni au Conseil d'État ni à l'ancienne Commission de protection de la vie privée, ayant tous deux appelé à un contenu obligatoire et non pas optionnel[26]. Le Conseil d'État voit dans le caractère facultatif du contenu du protocole tant une insécurité juridique qu'une contradiction au principe constitutionnel de légalité. À l'instar de la Commission de protection de la vie privée, il défend une définition précise du contenu du protocole[27].

À cette objection, le législateur répond que le principe de légalité renvoie en réalité à une base légale nationale ou supranationale amenant une autorité publique à collecter et traiter des données à caractère personnel pour remplir adéquatement ses missions de services publics[28]. À cet égard, l'article 6.3 du RGPD dispose que : « Les finalités du traitement sont définies dans cette base juridique ou en ce qui concerne le traitement visé au paragraphe 1, point e), sont nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Cette base juridique peut contenir des dispositions spécifiques pour adapter l'application des règles du présent règlement, entre autres : les conditions générales régissant la licéité du traitement par le responsable du traitement ; les types de données qui font l'objet du traitement ; les personnes concernées ; les entités auxquelles

25 CPVP, avis n° 33/2018 concernant l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, 11 avril 2018, p. 45, § 155.

26 CPVP, avis n° 33/2018 concernant l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, 11 avril 2018 p. 46, § 160 : « Quant au contenu du protocole, tel que l'article 22 en projet l'organise ; outre le fait que le législateur doit prévoir ses éléments obligatoires et non optionnels ("peut" doit être remplacé par "droit"),(…) ». Voy. également avis de la section de législation du Conseil d'État précédent la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, p. 21 « S'il est vrai que, du point de vue de la proportionnalité du transfert de données, le protocole peut être considéré comme une garantie procédurale utile étant donné qu'il amène les responsables de traitements à examiner au cas par cas le respect des exigences applicables aux transferts de données envisagés et à fixer explicitement les balises du transfert et que, de cette manière également, la transparence des traitements de données dans l'administration pourra être renforcée, le règlement de cette question par l'avant-projet ne satisfait pas à l'exigence de légalité dès lors, d'une part, que le protocole n'est pas rendu obligatoire alors qu'il devrait l'être et que, d'autre part, l'avant-projet n'énonce pas, de manière suffisamment précise, les différents éléments sur lesquels doivent porter ces protocoles ».

27 Avis de la section de législation du Conseil d'État précédent la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, p. 21, « (…) le règlement de cette question par l'avant-projet ne satisfait pas à l'exigence de légalité dès lors, d'une part, que le protocole n'est pas rendu obligatoire alors qu'il devrait l'être et que, d'autre part, l'avant-projet n'énonce pas, de manière suffisamment précise, les différents éléments sur lesquels doivent porter ces protocoles ».

28 Voy. projet de loi du 11 juin 2018 relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, Exposé des motifs, *Doc. parl.*, Ch. repr., 2017-2018, n° 54-3126/001, pp. 45 et s.

les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être ; la limitation des finalités ; les durées de conservation ; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, telles que celles prévues dans d'autres situations particulières de traitement comme le prévoit le chapitre IX. Le droit de l'Union ou le droit des États membres répond à un objectif d'intérêt public et est proportionné à l'objectif légitime poursuivi ». Or, toujours d'après le législateur, contrairement à une base légale, le protocole est quant à lui destiné à encadrer un échange particulier[29]. Malgré un second positionnement de l'ancienne CPVP interpellant le législateur fédéral sur l'inefficacité du protocole causée par son contenu optionnel et dénonçant une entrave au principe de légalité[30], la version définitive de la loi conserve le terme « pouvoir ».

Si l'objectif de facilitation des transferts de données à caractère personnel est louable, il nous semble que sa réalisation risque d'être mise en péril car le contenu des protocoles est laissé à la libre appréciation des autorités publiques concernées. À cet égard, on note l'absence de concordance avec la réglementation décrétale flamande, cette dernière fixant le contenu du protocole[31].

Les différentes mentions recommandées dans le protocole renvoient aux principes généraux applicables à tout traitement de données.

a. Le principe de licéité, loyauté et transparence

Les exigences de loyauté et de transparence ont pour principal objectif d'empêcher toute collecte et toute manipulation de données à caractère personnel obscures, imprévisibles ou secrètes pour les personnes concernées. Le respect de ces principes est primordial pour que se noue et perdure une relation de confiance entre les autorités publiques et les citoyens[32]. À cet égard, la Cour de justice de

29 Voy. projet de loi du 11 juin 2018 relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, Exposé des motifs, *Doc. parl.*, Ch. repr., 2017-2018, n° 54-3126/001, p. 45 : « Par base légale, il faut entendre tout texte de loi national ou supranational qui peut amener une administration à devoir traiter des données pour remplir ses missions au sens large. Ainsi, il ne faut pas entendre par base légale un texte qui prescrirait spécifiquement un traitement de données ou un transfert de données, mais plus généralement une disposition légale qui ne peut être réalisée autrement qu'en traitant des données. De même, la finalité doit être précise. Il faut entendre une fin en soi, et ne pas se limiter à la mention « exécution des missions légales de l'autorité publique ».

30 CPVP, avis n° 52/2018 concernant l'analyse du suivi de l'avis n° 33/2018 du 11 avril 2018 de la Commission de la protection de la vie privée et du projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel déposé à la Chambre des représentants le 11 juin 2018 (CO-A-2018-049), 22 juin 2018, p. 16, § 60 : « Toutefois, l'objet dudit protocole, qui est déterminé par l'article 20, § 1er, al. 2, reste facultatif. Cela rend totalement inefficace l'obligation de protocole insérée par l'alinéa 1er et cela amoindrit fortement la plus-value du système de protocole en termes d'outil d'*accountability* pour les responsables de traitements publics ; ce qui contrevient également au principe de légalité des traitements du secteur public ».

31 Decreet houdende de aanpassing van de decreten aan de verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (algemene verordening gegevensbescherming), *B.S.*, 26 juni 2018, p. 5172 ; CPVP, avis n° 52/2018 concernant l'analyse du suivi de l'avis n° 33/2018 du 11 avril 2018 de la Commission de la protection de la vie privée et du projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel déposé à la Chambre des représentants le 11 juin 2018 (CO-A-2018-049), 22 juin 2018, p. 16, § 61.

32 C. de Terwangne, « Internet et la protection de la vie privée et des données à caractère personnel », in *L'Europe des droits de l'homme à l'heure d'internet*, Q. Van Enis et C. de Terwangne (dir.), Bruxelles, Larcier, 2019, p. 342. Voy. également E. Degrave, « Le règlement général sur la protection des données et le

l'Union européenne a eu l'occasion, dans l'arrêt *Smaranda Bara e.a.*[33], d'insister sur la nécessité d'un comportement loyal de la part des responsables du traitement dans le cadre d'échange de données à caractère personnel entre deux organismes publics.

L'affaire au principal portait sur la contestation, par les personnes concernées, du transfert des données fiscales relatives à leurs revenus au regard de feue la directive 95/46/CE[34]. Ledit transfert était matérialisé par la conclusion d'un protocole interne entre les deux organismes publics, sans le consentement des personnes concernées et sans aucune information préalable. Les requérants soulevaient à la fois une violation du principe de finalité et du principe de transparence. Aux yeux de la Cour, la transmission initiale et le traitement subséquent par l'organisme récipiendaire entrent tous deux dans la notion de « traitement de données à caractère personnel »[35]. En effet, tant la directive 95/46/CE que le RGPD définissent la notion de « traitement » comme étant : « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données »[36]. En outre, la communication par transmission était déjà donnée à titre d'illustration par la directive 95/46/CE. S'agissant effectivement d'un traitement à caractère personnel, la Cour base principalement son raisonnement sur les articles 6, 10 et 13 de la directive.

Comme tout traitement de données à caractère personnel, le transfert d'informations fiscales doit respecter les principes de l'article 6, à savoir le principe de loyauté, de finalité, de nécessité, d'exactitude et de conservation limitée[37]. Ces principes restent d'application suite à l'entrée en vigueur du RGPD[38].

À l'estime de la Cour, le principe de loyauté est étroitement lié au respect de l'article 10 consacrant une obligation d'information pour le responsable du traitement. En effet, l'ancien article 10 énumérait les informations que le responsable du traitement devait obligatoirement communiquer à la personne concernée préalablement à tout traitement. Des informations additionnelles étaient prévues dans la mesure où celles-ci étaient nécessaires pour assurer, à l'égard de la personne concernée, un traitement loyal des données. La Cour relève que : « l'exigence de traitement loyal des données personnelles prévue à l'article 6 de la directive 95/46 oblige une administration

secteur public », *Rev. dr. commun.*, 2018 ; Groupe de l'Article 29, Guidelines on transparency under Regulation 3016/679, revised and adopted on 11 April 2018, WP 260rev01.

33 C.J.U.E., 1er octobre 2015, *Smaranda Bara e.a.*, C-201/14. Pour un bref commentaire, voy. notamment C. de Terwangne, « Internet et la protection de la vie privée et des données à caractère personnel », in *L'Europe des droits de l'homme à l'heure d'internet*, Q. Van Enis et C. de Terwangne (dir.), Bruxelles, Larcier, 2019, p. 345 ; C. Fievet, L. Gérard, N. Gillard, M. Knockaert, A. Michel, J. Mont, K. Rosier, T. Tombal et O. Vanreck, « Droit au respect de la vie privée et à la protection des données en lien avec les technologies de l'information », in *Chronique de jurisprudence en droit des technologies de l'information : 2015-2017*, *R.D.T.I.*, 2017, nos 68-69, p. 116, n° 139. A. Lachapelle, « Le respect du droit à la vie privée dans les traitements d'informations à des fins fiscales : état des lieux de la jurisprudence européenne (2e partie) », *R.G.F.C.P.*, 2016, n° 10, p. 58.

34 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, *J.O.*, L 281, du 23 novembre 1995, p. 0031 (ci-après « directive 95/46/CE »).

35 C.J.U.E., 1er octobre 2015, *Smaranda Bara e.a.*, C-201/14, point 29.

36 Article 2.2 de la directive 95/46/CE et article 4.2 du RGPD.

37 C.J.U.E., 1er octobre 2015, *Smaranda Bara e.a.*, C-201/14, point 30. A. Lachapelle, « Le respect du droit à la vie privée dans les traitements d'informations à des fins fiscales : état des lieux de la jurisprudence européenne (2e partie) », *op. cit.*, p. 65.

38 Article 5 du RGPD.

publique à informer les personnes concernées de la transmission de ces données à une autre administration publique en vue de leur traitement par cette dernière en sa qualité de destinataire desdites données »[39].

Relevons que désormais l'article 5.1 a), du RGPD prévoit que les données doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée. Les auteurs de la réglementation accordent dès lors une place à part entière à l'obligation de transparence, celle-ci n'étant plus assimilée à l'exigence de loyauté de la part du responsable de traitement. Les articles 12 à 14 du RGPD consacrent le devoir d'information de la part du responsable du traitement.

À l'absence d'information invoquée par les requérants, la partie défenderesse a brandi la loi nationale roumaine disposant que les données nécessaires à l'établissement de la qualité d'assuré sont transmises aux caisses d'assurances maladie par les autorités, sur la base d'un protocole. Toutefois, d'après la Cour, « il ressort des explications fournies par la juridiction de renvoi que les données nécessaires à l'établissement de la qualité d'assuré, au sens de ladite disposition, n'incluent pas celles relatives aux revenus, la loi reconnaissant également la qualité d'assuré aux personnes sans revenus imposables »[40]. Sur la base de ces éléments, la Cour considère que les personnes concernées ne pouvaient légitimement pas savoir que ces informations seraient également communiquées. Par conséquent, la disposition nationale ne constitue pas une information suffisante[41].

La Cour poursuit son analyse par l'applicabilité de l'article 13 de la directive permettant aux États membres de prendre des mesures législatives visant à limiter notamment la portée des obligations contenues à l'article 10.

La Cour relève que, la disposition nationale en cause ne concernant que la transmission d'informations, les exigences de l'article 13 ne sont pas remplies. En effet, elle n'apporte aucune précision sur les dérogations aux obligations d'information au bénéfice du responsable du traitement, ne remplissant dès lors pas l'exigence de prévisibilité de la norme[42].

Notons que le RGPD laisse également la possibilité aux législateurs nationaux de limiter, dans certaines circonstances, la portée de l'obligation d'information. Si la liste des situations permettant cette limitation est enrichie par la nouvelle réglementation, le RGPD prévoit que ces mesures législatives doivent contenir au moins des dispositions relatives aux finalités du traitement ou des catégories de traitement, aux catégories de données à caractère personnel, à l'étendue des limitations introduites, aux garanties destinées à prévenir les abus ou l'accès ou le transfert illicites, à la détermination du responsable du traitement ou des catégories de responsables du traitement, aux durées de conservation et aux garanties applicables ainsi

39 C.J.U.E., 1er octobre 2015, *Smaranda Bara e.a.*, C-201/14, point 34.

40 C.J.U.E., 1er octobre 2015, *Smaranda Bara e.a.*, C-201/14, point 37.

41 C.J.U.E., 1er octobre 2015, *Smaranda Bara e.a.*, C-201/14, points 37-38. De surcroît, soulignons l'importance accordée par la jurisprudence européenne et belge à la communication aux personnes concernées de leur droit d'accès et de rectification afin qu'elles puissent exercer l'ensemble des droits accordés par le RGPD ; voy. notamment C.J.U.E. (3e ch.), 1er octobre 2015, *Smaranda Bara,* C-201/14, point 33 ; C.J.U.E. (2e ch.), 20 décembre 2017, *Peter Nowak c. Data Protection Commissionner*, C-434/16, point 48 ; C. trav. Liège (6e ch.), 6 février 2015, *J.T.T.*, 2015/29, p. 299. Pour une analyse approfondie, voy. C. Fievet, L. Gérard, N. Gillard, M. Knockaert, A. Michel, J. Mont, K. Rosier, T. Tombal et O. Vanreck, « Droit au respect de la vie privée et à la protection des données en lien avec les technologies de l'information », in *Chronique de jurisprudence en droit des technologies de l'information : 2015-2017*, H. Jacquemin et T. Tombal (coord.), *R.D.T.I.*, 2017, nos 68-69, p. 102, p. 106, p. 109, p. 114, p. 116.

42 C.J.U.E., 1er octobre 2015, *Smaranda Bara e.a.*, C-201/14, points 40-41.

qu'aux risques pour les droits et libertés des personnes concernées. De plus, les personnes concernées doivent en principe être informées de la limitation[43].

Dans l'arrêt *Smaranda Bara e.a.,* la Cour pointe l'absence d'information dans le chef de l'organisme public recevant les informations transmises[44].

En ce qui concerne le droit belge, mentionnons que le protocole actuellement mis en place par le législateur fédéral contient encore à nos yeux des écueils[45]. Certes, les mentions d'identification du responsable du traitement qui transfère les données à caractère personnel et d'identification du responsable du traitement destinataire de celles-ci ainsi que les coordonnées des délégués à la protection des données concernées tant de la part de l'entité émettrice que de l'entité participent à l'exigence de transparence. La loi prévoit également d'indiquer les catégories de données à caractère personnel faisant l'objet du transfert. Nonobstant cette première observation, nous estimons que ces catégories devraient être suffisamment précises pour permettre un contrôle réel par les personnes concernées et doivent faire l'objet d'une publicité effective et efficace. En outre, il est à craindre que l'idéal de loyauté souffre du caractère non contraignant du contenu du protocole.

b. Le principe de limitation des finalités

En substance, l'article 5.1 b) du RGPD impose une collecte de données à caractère personnel pour des finalités déterminées, explicites et légitimes et interdit tout traitement ultérieur qui serait incompatible avec la ou les finalité(s) d'origine. Du principe de finalité découle l'étude de ce que le responsable du traitement peut faire ou ne pas faire avec les données à caractère personnel, les données qu'il/elle peut traiter et leur durée de conservation[46].

Lorsque le responsable du traitement à qui les données à caractère personnel sont transférées ne poursuit pas la même finalité que celle poursuivie par le responsable du traitement originaire, ce second traitement est considéré comme un traitement ultérieur soumis à l'examen de compatibilité[47].

L'article 6.4 du RGPD établit une liste de cinq critères à prendre en compte par le responsable du traitement pour vérifier si le traitement envisagé est compatible avec le traitement pour lequel les données ont été collectées à l'origine. Il est exigé du responsable du traitement de tenir compte de l'existence éventuelle d'un lien entre les finalités pour lesquelles les

43 Article 23 du RGPD. Sur la limitation des droits de la personne concernée, voy. T. Tombal, « Les droits de la personne concernée dans le RGPD », in *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie* (C. de Terwangne et K. Rosier, dir.), 1re éd., coll. du CRIDS, Bruxelles, Larcier, 2018, pp. 540 et s.

44 C.J.U.E., 1er octobre 2015, *Smaranda Bara e.a.*, C-201/14, point 44.

45 Voy. également les critiques émises par Élise Degrave ; E. Degrave, « Protection des données et comités sectoriels : avant et après le RGDD », note sous C. const., 8 novembre 2018, *R.D.T.I.*, 2018/4, n° 73, pp. 91-97.

46 À ce propos, voy. C. de Terwangne, « Les principes relatifs au traitement des données à caractère personnel et à sa licéité », in *Le règlement général sur la protection des données (RGPD/GDPR) – Analyse approfondie*, C. de Terwangne et K. Rosier (coord.), Bruxelles, Larcier, pp. 94 et s.

47 Voy. C. de Terwangne, « Les principes relatifs au traitement des données à caractère personnel et à sa licéité », in *Le règlement général sur la protection des données (RGPD/GDPR) – Analyse approfondie*, C. de Terwangne et K. Rosier (coord.), Bruxelles, Larcier, pp. 98 et s. Dans son avis portant sur l'avant-projet de loi du 30 juillet 2018, l'ancienne CPVP avait d'ailleurs précisé que le protocole n'amenait pas nécessairement un traitement ultérieur de données et pouvait s'inscrire dans la poursuite de la finalité initiale ; CPVP, avis n° 33/2018 concernant l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, 11 avril 2018, p. 46, § 159.

données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé, du contexte dans lequel les données ont été collectées, de leur nature, des conséquences possibles du traitement ultérieur pour les personnes concernées et de l'existence de garanties appropriées.

Soulignons que le protocole oblige les responsables du traitement à indiquer les finalités pour lesquelles les données à caractère personnel sont transférées en *sus* de la base légale sur laquelle repose le transfert. Relevons que le législateur n'a pas intégré la recommandation de l'ancienne CPVP selon laquelle la loi devait prévoir à la fois la base légale qui fonde le transfert, mais également celle sur laquelle repose la réception ou la consultation des données[48].

Le Conseil d'État avait suggéré de préciser que l'exposé des finalités ne pouvait se limiter à l'expression de la nécessité de collecter les données à caractère personnel pour l'exercice des missions légales de l'autorité publique[49]. Cette recommandation n'a cependant pas été reprise dans la version finale de la loi.

c. *Le principe de minimisation des données*

L'article 5.1 c) du RGPD prévoit l'exigence d'une utilisation de données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

Cette obligation impose au responsable du traitement de s'interroger sur les données qui lui sont strictement nécessaires afin d'accomplir son objectif et de favoriser l'utilisation de données anonymisées ou à tout le moins pseudonymisées. Relevons qu'une politique de minimisation ne s'applique, en réalité, pas uniquement à la quantité de données collectées, mais également au nombre de personnes pouvant traiter les données et à la durée de conservation. En outre, le principe de minimisation vise également à vérifier la qualité des données et à privilégier les informations les moins intrusives possible pour accomplir la finalité[50].

Le principe de minimisation se trouve consacré dans le protocole en ce qu'il doit prévoir les catégories de données à caractère personnel transférées et leur format[51] ainsi que les catégories de destinataires. À titre d'exemple, l'Autorité de protection des données a incité à la conclusion d'un tel protocole entre la banque de données fédérale « e-PV »[52] et une autorité régionale[53].

48 CPVP, avis n° 52/2018 concernant l'analyse du suivi de l'avis n° 33/2018 du 11 avril 2018 de la Commission de la protection de la vie privée et du projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel déposé à la Chambre des représentants le 11 juin 2018 (CO-A-2018-049), 22 juin 2018, p. 17, § 64, b).

49 Avis de la section de législation du Conseil d'État précédent la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, p. 68616, p. 22.

50 C. de Terwangne, K. Rosier et B. Losdyck, « Le règlement européen relatif à la protection des données à caractère personnel : quelles nouveautés ? », *J.D.E.*, 2017, p. 25.

51 L'insertion du format des données provient d'une recommandation de la CPVP (désormais APD) ; CPVP, avis n° 33/2018 concernant l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, 11 avril 2018, p. 46, § 160, b).

52 https://www.ucm.be/Actualites/Droit-penal-social-un-proces-verbal-electronique-uniforme2.

53 APD, avis n° 168/2018 sur le projet d'arrêté du gouvernement wallon relatif au contrôle des législations et réglementations relatives à la reconversion et au recyclage professionnels ainsi qu'à l'instauration d'amendes administratives applicables en cas d'infraction à ces législations et réglementations et sur le projet d'arrêté du gouvernement wallon relatif au contrôle des législations et réglementations relatives à la politique économique, à la politique de l'emploi et à la recherche scientifique ainsi qu'à l'instauration d'amendes administratives applicables en cas d'infraction à ces législations et réglementations, 19 décembre 2018. À propos de la nécessité de conclure un protocole, voy. également APD, avis n° 130/2018 concernant l'avant-projet d'arrêté du

d. Le principe d'intégrité et de confidentialité

L'article 5.1 f) du RGPD dispose que les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques et/ou organisationnelles appropriées[54].

À la lumière du principe d'intégrité et de confidentialité, érigé au rang de principe clé, le protocole prévoit la mention des modalités de communication utilisées ainsi que de toute mesure spécifique encadrant le transfert conformément au principe de proportionnalité et aux exigences de protection des données dès la conception et par défaut. L'ancienne CPVP précise que sont uniquement visées les mesures de sécurité encadrant le transfert des informations entre l'autorité publique fédérale et l'autorité publique ou privée récipiendaire. Elle appelle également à la vigilance. En effet, le protocole ayant vocation à être porté à la connaissance de tous, les mesures de sécurité devraient être décrites de manière fonctionnelle afin d'éviter d'augmenter le risque d'attaque de sécurité[55].

e. Autre

Par ailleurs, l'article 20, alinéa 2, de la loi dispose que le protocole peut également prévoir les restrictions légales applicables aux droits de la personne concernée. Dans son second avis, l'ancienne CPVP avait recommandé d'inclure également la justification sur laquelle repose la restriction légale aux droits des personnes concernées. Le législateur n'a toutefois pas suivi la Commission sur ce point[56].

Notons également qu'à l'instar de la précédente directive 95/46/CE, le RGPD prévoit différentes hypothèses dans lesquelles le responsable du traitement est exonéré de l'exigence d'information. En effet, lorsque les données à caractère personnel sont collectées directement auprès de la personne concernée, le responsable du traitement n'est pas tenu au respect des exigences d'informations si celle-ci en dispose déjà[57]. En outre, la réglementation prévoit des hypothèses additionnelles dans lesquelles le responsable du traitement n'est pas tenu à la communication des informations lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée, notamment lorsque la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés ou encore lorsque les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union ou le droit national. Enfin, le responsable du traitement est exonéré de l'exigence d'informations lorsque « l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union ou le droit de l'État membre auquel le responsable de traitement est soumis et qui prévoit des mesures appropriées visant à protéger les

gouvernement flamand portant exécution de la loi du 30 avril 1999 relative à l'occupation des travailleurs étranger, 28 novembre 2018.

54 Sur l'exigence de sécurité, voy. F. Dumortier, « La sécurité des traitements de données, les analyses d'impact et les violations de données », in *Le règlement général sur la protection des données (RGPD/GDPR) – Analyse approfondie*, C. de Terwangne et K. Rosier (coord.), Bruxelles, Larcier, 2018, p. 143.

55 CPVP, avis n° 33/2018 concernant l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, 11 avril 2018, p. 46, § 160, d).

56 CPVP, avis n° 52/2018 concernant l'analyse du suivi de l'avis n° 33/2018 du 11 avril 2018 de la Commission de la protection de la vie privée et du projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel déposé à la Chambre des représentants le 11 juin 2018 (CO-A-2018-049), 22 juin 2018, p. 17, § 64, c).

57 Article 13.4 du RGPD.

intérêts légitimes de la personne concernée »[58]. À titre d'illustration, l'article 17 de la loi du 30 juillet 2017 consacre une telle exonération[59].

Relevons que plusieurs propositions de l'ancienne CPVP, appuyées par le Conseil d'État, n'ont, ici aussi, pas été prises en compte.

Premièrement, la CPVP était d'avis de prévoir la description des finalités précises pour lesquelles les données à caractère personnel avaient été collectées à l'origine[60].

Deuxièmement, la CPVP avait suggéré qu'en cas de traitement ultérieur des données[61], l'analyse de compatibilité de la nouvelle finalité avec celle poursuivie à l'origine lors de la collecte initiale soit mentionnée[62]. En effet, conformément à l'article 6.4 du RGPD, lorsque le traitement à une fin autre que celle pour laquelle les données ont été collectées n'est pas fondé sur le consentement de la personne concernée ou sur le droit de l'Union ou le droit national, le responsable du traitement doit s'assurer que ce traitement à une fin autre est compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées. Pour ce faire, le responsable du traitement qui prévoit de transférer les informations doit tenir compte de plusieurs critères, à savoir de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé, du contexte dans lequel les données ont été collectées, de la nature de celles-ci, des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ainsi que de l'existence de garanties appropriées comme notamment le chiffrement ou la pseudonymisation. En revanche, le législateur considère que la mention de l'analyse de compatibilité des finalités en cas de traitement ultérieur est en contradiction avec l'exigence de base légale[63].

Troisièmement et enfin, la CPVP avait également soulevé qu'il convenait d'ajouter la vérification du respect du principe de collecte auprès de la source authentique des données, ce qui garantit la qualité des données à caractère personnel

58 Article 14.5 du RGPD. Nous attirons l'attention du lecteur sur les articles 11 à 17 de la loi du 30 juillet 2018 à propos de la limitation des droits des personnes concernées.

59 L'article 17 de la loi du 30 juillet 2018 dispose que « En application de l'article 23 du Règlement, un responsable du traitement visé au présent titre qui communique des données à caractère personnel à une banque de données conjointe ne peut informer la personne concernée de cette transmission. Par « banque de données conjointe », on entend l'exercice commun des missions effectuées dans le cadre du titre 1er et des titres 2 ou 3 par plusieurs autorités, structurée à l'aide de procédés automatisés et appliqués aux données à caractère personnel ».

60 CPVP, avis n° 33/2018 concernant l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, 11 avril 2018, p. 47, § 160, h) ; avis n° 52/2018 concernant l'analyse du suivi de l'avis n° 33/2018 du 11 avril 2018 de la Commission de la protection de la vie privée et du projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel déposé à la Chambre des représentants le 11 juin 2018 (CO-A-2018-049), 22 juin 2018, p. 17, § 64, d).

61 Sur la notion de traitement ultérieur, voy. C. de Terwangne, « Les principes relatifs au traitement des données à caractère personnel et à sa licéité », in *Le règlement général sur la protection des données (RGPD/GDPR) – Analyse approfondie*, C. de Terwangne et K. Rosier (coord.), Bruxelles, Larcier, 2018, pp. 98-102.

62 CPVP, avis n° 33/2018 concernant l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, 11 avril 2018, p. 47, § 160, h) ; avis n° 52/2018 concernant l'analyse du suivi de l'avis n° 33/2018 du 11 avril 2018 de la Commission de la protection de la vie privée et du projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel déposé à la Chambre des représentants le 11 juin 2018 (CO-A-2018-049), 22 juin 2018, p. 17, § 64, d).

63 Voy. projet de loi du 11 juin 2018 relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, Exposé des motifs, *Doc. parl.*, Ch. repr., 2017-2018, n° 54-3126/001, p. 45.

transférées[64]. De manière laconique, le législateur justifie le refus de l'insertion de cette précision par le fait qu'une telle exigence n'est pas essentielle lorsqu'une base légale existe et ne découle pas du RGPD[65]. Cette justification paraît critiquable. En effet, l'exactitude des données est un des principes de base de la législation relative à la protection des données à caractère personnel. À l'instar de l'obligation prévalant sous l'égide de la directive 95/46/CE, l'article 5 du RGPD dispose que les données doivent être exactes et, si nécessaire, tenues à jour. Toutes les mesures raisonnables doivent être prises pour que les informations qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder. Notons que l'ancienne directive 95/46/CE exigeait que des mesures raisonnables soient également prises pour l'effacement ou la correction de données incomplètes au regard de la finalité poursuivie. Cette précision ne figure pas dans l'article 5 du RGPD relatif aux principes du traitement, mais se trouve consacrée à l'article 16 prévoyant un droit de rectification pour la personne concernée[66].

Le simple fait que le traitement repose sur une base légale n'exempte pas le responsable du traitement du respect de ce principe d'exactitude. En outre, le mécanisme de collecte unique auprès d'une source authentique étant propre à la Belgique, il semble logique que le RGPD reste muet sur le sujet. Par ailleurs, il semble contradictoire d'invoquer une norme européenne pour un texte ayant vocation à appliquer cette norme aux particularismes nationaux.

4. Publicité du protocole

En son article 32, la Constitution consacre le principe de transparence administrative : « Chacun a le droit de consulter chaque document administratif et de s'en faire remettre copie, sauf dans les cas et conditions fixés par la loi, le décret ou la règle visée à l'article 134 ». Le législateur belge a également entériné ce principe dans la loi du 11 avril 1994 sur la publicité de l'administration[67]. Tant une publicité active que passive sont promues. En effet, l'article 2 oblige les autorités administratives fédérales[68] à participer activement à la transparence en fournissant aux citoyens une information claire et objective sur leurs actions. Par ailleurs, le chapitre trois de la loi consacre et organise la publicité passive octroyant, sous réserve d'ex-

64 CPVP, avis n° 33/2018 concernant l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, 11 avril 2018, p. 47, § 160, h) ; avis n° 52/2018 concernant l'analyse du suivi de l'avis n° 33/2018 du 11 avril 2018 de la Commission de la protection de la vie privée et du projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel déposé à la Chambre des représentants le 11 juin 2018 (CO-A-2018-049), 22 juin 2018, p. 17, § 64, d).

65 Voy. projet de loi du 11 juin 2018 relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, Exposé des motifs, *Doc. parl.*, Ch. repr., 2017-2018, n° 54-3126/001, p. 45.

66 À ce propos, voy. C. de Terwangne, « Les principes relatifs au traitement des données à caractère personnel et à sa licéité », in *Le règlement général sur la protection des données (RGPD/GDPR) – Analyse approfondie*, C. de Terwangne et K. Rosier (coord.), Bruxelles, Larcier, 2018, p. 112.

67 Loi du 11 avril 1994 relative à la publicité de l'administration, *M.B.*, 30 juin 1994 ; p. 17662 ; E. Degrave, « Le règlement général sur la protection des données et le secteur public », *Rev. dr. commun.*, 2018, pp. 4-5. Voy. également E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, Bruxelles, Larcier, 2014.

68 L'article 1er de la loi du 11 avril 1994 dispose que « La présente loi s'applique a) aux autorités administratives fédérales b) aux autorités administratives autres que les autorités administratives fédérales, mais uniquement dans la mesure où, pour des motifs relevant des compétences fédérales, la présente loi interdit ou limite la publicité de document administrative ». L'article 1er, alinéa 2, 1° définit également l'autorité administrative comme « une autorité administrative visée à l'article 14 de lois coordonnées sur le Conseil d'État ».

ceptions, le droit de consulter un document administratif[69].

À l'heure du numérique, dans son avis portant sur la loi du 30 juillet 2018, le Conseil d'État modernise le concept de transparence en indiquant que : « Dans le contexte de l'administration électronique fondée sur la collecte unique des données, il y a lieu de considérer que le droit fondamental à la transparence administrative suppose que toute personne doit pouvoir accéder à une vue d'ensemble de la localisation des données détenues par les autorités publiques et de leur utilisation pour comprendre l'environnement administratif dans lequel elle se trouve »[70]. Une telle conception est cruciale dans le contexte administratif belge actuel dans lequel le principe de collecte unique amène à une forte circulation des informations et à un nombre croissant d'intervenants bouleversant quotidiennement le paysage informationnel numérique[71].

Afin d'assurer la prévisibilité et l'accessibilité de la circulation des données à caractère personnel, la CPVP[72] et le Conseil d'État[73] avaient appelé à une publicité active des protocoles conclus. La CPVP envisageait l'utilisation d'un portail Internet où, sous condition d'authentification préalable, les citoyens peuvent voir, pour les données les concernant, leur circulation au sein des autorités publiques avec les finalités mentionnées, contrôler les utilisations, corriger les éventuelles erreurs informationnelles et, enfin, entrer facilement en contact avec le délégué à la protection des données de l'autorité publique ayant reçu les données à caractère personnel les concernant. Le législateur n'a néanmoins pas suivi l'ancienne CPVP et le Conseil d'État sur ce point[74].

Désormais, l'article 20, § 3, de la loi prévoit la publication du protocole sur les sites Internet des responsables du traitement concernés par le transfert. Relevons toutefois que l'ancienne CPVP, dans son second avis, avait requis une publication officielle au *Moniteur belge*[75].

Des craintes, que nous partageons, émergent quant à l'accessibilité aux informations par les citoyens au regard de la multitude d'acteurs concernés[76].

69 L'article 1er, alinéa 2, 2°, de la loi du 11 avril 1994 définit largement le document administratif comme « toute information, sous quelque forme que ce soit, dont une autorité administrative dispose ».

70 Avis de la section de législation du Conseil d'État précédent la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, p. 68616, p. 24.

71 À ce propos, voy. E. Degrave, *L'e-Gouvernement et la protection de la vie privée : Légalité, transparence et contrôle,* Bruxelles, Larcier, 2014. Voy. également de la même auteure « L'administration belge organisée en réseaux : réutilisation des données à caractère personnel et protection de la vie privée », *op. cit.*, pp. 189-190.

72 CPVP, avis n° 33/2018 concernant l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, 11 avril 2018, p. 50, § 171.

73 Avis de la section de législation du Conseil d'État précédent la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, p. 68616, p. 23.

74 Voy. à ce sujet CPVP, avis n° 52/2018 concernant l'analyse du suivi de l'avis n° 33/2018 du 11 avril 2018 de la Commission de la protection de la vie privée et du projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel déposé à la Chambre des représentants le 11 juin 2018 (CO-A-2018-049), 22 juin 2018, p. 18, § 67.

75 CPVP, avis n° 52/2018 concernant l'analyse du suivi de l'avis n° 33/2018 du 11 avril 2018 de la Commission de la protection de la vie privée et du projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel déposé à la Chambre des représentants le 11 juin 2018 (CO-A-2018-049), 22 juin 2018, p. 17, § 65.

76 C. de Terwangne, E. Degrave, A. Delforge et L. Gerard, *La protection des données à caractère personnel en Belgique : manuel de base*, Bruxelles, Politeia, 2019, p. 166. Pour des exemples d'initiatives, nous pouvons relever le protocole conclu entre le SPF Finances et FAMIFED (disponible sur https://finances.belgium.be/sites/default/files/Privacy/

5. Rôle du DPO

Le RGPD a consacré le rôle du délégué à la protection des données (plus connu sous son acronyme anglais « DPO »). En substance, le DPO a pour principales fonctions d'assurer le respect de la réglementation au sein de l'autorité publique ou d'une entité privée, d'apporter son aide dans la mise en place du RGPD, d'informer et d'élaborer des recommandations, de coopérer avec l'autorité de contrôle et, enfin, il a vocation à constituer le point de contact entre l'autorité publique ou l'entité privée et les personnes concernées[77].

Le RGPD rend sa désignation obligatoire dans trois circonstances.

Premièrement, les autorités publiques sont tenues de compléter leur équipe d'un délégué à la protection des données. L'importance des traitements ainsi que la quantité et la qualité des données à caractère personnel traitées n'a pas d'incidence[78].

Deuxièmement, un DPO est obligatoire lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées[79].

Troisièmement et enfin, la désignation d'un DPO est encore obligatoire quand les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées aux articles 9 et 10 de la réglementation européenne[80].

Lors de l'implémentation du RGPD, le législateur belge a prévu une autre hypothèse portant obligation de nommer un délégué à la protection des données. L'article 21 dispose qu'un organisme privé (et non plus public, contrairement à la situation prévalant sous l'égide du règlement) qui, en sa qualité de sous-traitant, traite des données à caractère personnel pour le compte d'une autorité publique fédérale ou à qui une autorité publique fédérale a transféré des données à caractère personnel doit nommer un DPO. Il semble que l'objectif de la loi ait été de prévoir la promotion du délégué au sein du secteur privé lorsqu'il intervient dans la chaîne de traitement de données à caractère personnel issues du secteur public.

Cette obligation est toutefois imposée uniquement lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques[81].

Protocole%20SPF%20FIN-Famifed-2018-316-FR.pdf) et celui conclu entre le SPF et la DGO Fiscalité (disponible sur https://www.wallonie.be/sites/default/files/2019-07/protocole_17.pdf).

77 Pour une analyse plus détaillée, voy. K. Rosier, « Délégué à la protection des données : une fonction multifacette », in *Le règlement général sur la protection des données (RGPD/GDPR) – Analyse approfondie*, C. de Terwangne et K. Rosier (coord.), Bruxelles, Larcier, pp. 559-592. Voy. également C. de Terwangne, E. Degrave, A. Delforge et L. Gerard, *La protection des données à caractère personnel en Belgique : manuel de base*, Bruxelles, Politeia, 2019.

78 Article 37.1 a), du RGPD.

79 Article 37.1 b), du RGPD. Pour une concrétisation de la notion, voy. Groupe de l'Article 29, Lignes directrices du 13 décembre 2016 concernant les délégués à la protection des données (DPD), WP 243, révisées le 5 avril 2017, p. 8 ; C. de Terwangne, E. Degrave, A. Delforge et L. Gerard, *La protection des données à caractère personnel en Belgique : manuel de base*, Bruxelles, Politeia, 2019, p. 91.

80 Article 37.1. c), du RGPD. Pour une concrétisation de la notion, voy. Groupe de l'Article 29, Lignes directrices du 13 décembre 2016 concernant les délégués à la protection des données (DPD), WP 243, révisées le 5 avril 2017, p. 8 ; C. de Terwangne, E. Degrave, A. Delforge et L. Gerard, *La protection des données à caractère personnel en Belgique : manuel de base*, 2019, Bruxelles, Politeia, p. 91.

81 Le législateur fait référence à l'article 35 du RGPD. Notons que le législateur belge impose également la désignation d'un DPO pour le responsable de traitement qui désire bénéficier du régime dérogatoire prévu au titre 4 de la loi du 30 juillet 2018 en cas de risque élevé ; article 190 de la loi du 30 juillet 2018.

Dans les autres cas, une désignation volontaire d'un délégué à la protection des données est possible et fortement recommandée[82]. En effet, le DPO a pour fonction d'informer et de conseiller le responsable du traitement, ses sous-traitants et ses employés des obligations relatives à la protection des données à caractère personnel. Il a également pour missions de contrôler le respect de la réglementation et de coopérer avec l'autorité de contrôle[83]. Par ailleurs, afin d'éviter tout conflit d'intérêts, le RGPD insiste sur son indépendance hiérarchique et fonctionnelle[84].

L'article 20, § 2, de la loi belge prévoit que le protocole est adopté après les avis respectifs du délégué à la protection des données de l'autorité publique fédérale détenteur des données à caractère personnel et du destinataire. Leurs avis ne sont pas contraignants. Toutefois, si au moins un des avis n'est pas suivi par le responsable du traitement, il doit motiver sa décision et reprendre les motifs dans les dispositions introductives du protocole.

À la lecture des travaux préparatoires de la loi et de ses dispositions, une zone d'ombre semble se dessiner. En effet, l'article 20 exige que le protocole soit soumis aux avis respectifs tant du délégué à la protection des données de l'autorité publique transférant les données que du destinataire. La loi ne prévoit à cet égard aucune exception. Cependant, l'article 21, quant à lui, ne semble rendre obligatoire la désignation d'un délégué à la protection des données pour un organisme privé à qui les données ont été transférées uniquement en cas de risque élevé pour les droits et libertés des personnes concernées. La limitation d'une nomination obligatoire d'un DPO en cas de risque élevé pour les personnes concernées pourrait s'expliquer par le souci du législateur de répondre à une objection soulevée par l'ancienne CPVP dans son avis portant sur l'avant-projet de loi. En effet, l'organe de contrôle belge avait considéré que le recours automatique au délégué à la protection des données pour chacun des traitements ne correspondait pas à l'approche par le risque promu par la réglementation européenne. L'ancienne CPVP se rallie aux propos du Groupe de l'Article 29[85] qui appelait les délégués à la protection des données à établir des priorités dans leurs interventions[86].

Notons que le délégué à la protection des données est susceptible d'intervenir à plusieurs reprises. Son action est, en tous les cas, requise pour la conclusion d'un protocole de transfert entre deux autorités publiques ou entre un organisme public et une entité privée. Par ailleurs, l'article 22 de la loi prévoit aussi l'intervention du délégué lorsque le traitement (et non plus uniquement un transfert) de données à caractère personnel envisagé est susceptible d'engendrer un risque élevé pour les droits

82 À ce sujet, voy. C. de Terwangne, E. Degrave, A. Delforge et L. Gerard, *La protection des données à caractère personnel en Belgique : manuel de base*, 2019, Bruxelles, Politeia, p. 96.

83 Article 39 du RGPD ; C. de Terwangne, E. Degrave, A. Delforge et L. Gerard, *La protection des données à caractère personnel en Belgique : manuel de base*, Bruxelles, Politeia, 2019, p. 92 ; K. Rosier, « Délégué à la protection des données : une fonction multifacette », in *Le règlement général sur la protection des données (RGPD/GDPR) – Analyse approfondie*, C. de Terwangne et K. Rosier (coord.), Bruxelles, Larcier, 2018, pp. 559-592.

84 Article 38 du RGPD ; voy. C. de Terwangne, E. Degrave, A. Delforge et L. Gerard, *La protection des données à caractère personnel en Belgique : manuel de base*, 2019, Bruxelles, Politeia, pp. 94-95 ; K. Rosier, « Délégué à la protection des données : une fonction multifacette », in *Le règlement général sur la protection des données (RGPD/GDPR) – Analyse approfondie*, C. de Terwangne et K. Rosier (coord.), Bruxelles, Larcier, 2018, pp. 559-592.

85 Désormais devenu Comité européen de protection des données « EDPB ».

86 CPVP, avis n° 33/2018 concernant l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, 11 avril 2018, p. 51, § 174 ; Groupe de l'Article 29, Guidelines on Data Protection Officers ('DPOs'), revised and adopted on 5 April 2017, WP 243rev01, p. 22.

et libertés des citoyens. Lorsque l'autorité publique fédérale poursuit la mise en œuvre du traitement, contrairement à l'opinion du délégué à la protection des données, elle doit motiver sa décision[87].

Précisons également que l'ancienne CPVP avait suggéré l'implication du DPO dans le groupe d'experts originellement envisagé par le législateur fédéral. En effet, dans sa première version, la section relative au secteur public contenait un article 27 portant création d'un groupe d'experts composé de représentants des autorités publiques fédérales et des organismes publics fédéraux, éventuellement appuyés par des experts extérieurs. L'objectif était, non pas une substitution de l'autorité de contrôle nationale, mais la mise en place d'une « plateforme de concertation dans le cadre du développement de la politique relative à la protection des données au sein des autorités publiques fédérales et les organismes publics fédéraux »[88]. Tant le Conseil d'État[89] que l'ancienne CPVP[90] avaient appelé à plus de précision quant à sa composition et ses missions. Notons que la version définitive du texte de loi ne reprend pas cette disposition.

6. *Sanctions*

L'article 20 laisse le soin aux responsables du traitement concernés de déterminer les sanctions applicables en cas de non-respect d'une ou plusieurs obligations contenues dans le protocole, sans préjudice du titre 6 de la loi relatif aux sanctions administratives et pénales.

Cependant, nous pouvons nous interroger sur l'effectivité du titre 6 lorsque l'article 221, § 2, de la loi du 30 juillet 2018 exclut l'application de l'article 83 du RGPD[91] relatif aux conditions pour imposer des amendes administratives aux « autorités publiques et leurs préposés ou mandataires sauf s'il s'agit de personnes morales de droit public qui offrent des biens ou des services sur un marché ». Cette exonération n'a pas manqué d'interpeller le Conseil d'État qui a insisté sur la nécessité d'encadrer fermement les transferts de données, sous peine de souffrir d'« un grave retour en arrière sur le plan de la protection de la vie privée des citoyens »[92]. À cette objection, le législateur se défend par l'énumération de plusieurs arrêts de la Cour constitutionnelle reconnaissant qu'une différence de traitement entre les personnes morales, selon qu'elles disposent d'un organe démocratiquement élu ou non, repose sur un critère objectif[93]. Le législateur mentionne en particulier que : « la Cour

87 Article 22 de la loi du 30 juillet 2018.

88 Voy. l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *Doc. parl.*, Ch. repr., 2017-2018, n° 54-3126/001, p. 271.

89 Avis de la section de législation du Conseil d'État précédent la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, p. 68616, p. 25.

90 CPVP, avis n° 33/2018 concernant l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, 11 avril 2018, p. 51, § 175.

91 Pour plus d'informations au sujet des sanctions prévues par le RGPD, voy. L. Gerard, « Les sanctions en cas de non-respect du RGPD : vers une plus grande effectivité de la protection des données à caractère personnel ? », in *Le règlement général sur la protection des données (RGPD/GDPR) – Analyse approfondie*, C. de Terwangne et K. Rosier (coord.), Bruxelles, Larcier, 2018, pp. 641-654 ; L. Gerard, « RGPD : Quatre recours pour un règlement », in *Le règlement général sur la protection des données (RGPD/GDPR) – Analyse approfondie*, C. de Terwangne et K. Rosier (coord.), Bruxelles, Larcier, 2018, pp. 655-664.

92 Avis de la section de législation du Conseil d'État précédent la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, p. 68616, p. 21.

93 Voy. notamment Cour const., 10 juillet 2002, n° 128/2002, *M.B.*, 13 novembre 2002 ; Cour const., 21 février 2007, n° 31/2007, *M.B.*, 12 avril 2007 ; voy. projet de loi du 11 juin 2018 relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, Exposé des motifs, *Doc. parl.*, Ch. repr., 2017-2018, n° 54-3126/001, pp. 228-233.

constitutionnelle a, dans son arrêt 128/2002 du 10 juillet 2002, établit que "B.7.5. La différence de traitement ainsi établie entre personnes morales selon qu'elles disposent d'un organe démocratiquement élu ou non repose sur un critère objectif. Les personnes morales de droit public énumérées à l'article 5, alinéa 4, du Code pénal ont la particularité d'être principalement chargées d'une mission politique essentielle dans une démocratie représentative, de disposer d'assemblées démocratiquement élues et d'organes soumis à un contrôle politique. Le législateur a pu raisonnablement redouter, s'il rendait ces personnes morales pénalement responsables, d'étendre une responsabilité pénale collective à des situations où elle comporte plus d'inconvénients que d'avantages, notamment en suscitant des plaintes dont l'objectif réel serait de mener, par la voie pénale, des combats qui doivent se traiter par la voie politique"»[94].

C. Analyse d'impact

La réglementation européenne prévoit que lorsqu'un type de traitement, notamment en raison de sa nature, sa portée, son contexte et ses finalités, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, une analyse d'impact préalable est exigée[95]. Cependant, lorsque le traitement repose sur une base légale ou sur l'exercice d'une mission d'intérêt public, le législateur européen exonère le responsable du traitement d'une telle analyse d'impact si elle a été réalisée en amont, au moment de la discussion et de l'adoption de la base juridique autorisant le traitement des données à caractère personnel[96].

Toutefois, une marge de manœuvre est laissée aux États membres qui peuvent dès lors décider d'obliger le responsable du traitement à effectuer une seconde analyse d'impact. Le législateur belge s'est saisi de cette liberté. En effet, l'article 23 de la loi dispose qu'« En exécution de l'article 35.10 du règlement, une analyse d'impact spécifique de protection des données est effectuée avant l'activité de traitement, même si une analyse d'impact générale relative à la protection des données a déjà été réalisée dans le cadre de l'adoption de la base légale ».

La première analyse d'impact est donc générale et abstraite, permettant au législateur de décider s'il maintient son projet de base légale mettant en place des traitements de données à caractère personnel ou non, au regard des droits et libertés de ses citoyens. La seconde analyse d'impact, propre à la loi du 30 juillet 2018, intervient préalablement au traitement effectif par le responsable du traitement et rend possible une analyse plus concrète et casuistique[97]. Cette disposition est conforme à la recommandation de l'ancienne CPVP[98].

94 Voy. projet de loi du 11 juin 2018 relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, Exposé des motifs, *Doc. parl.*, Ch. repr., 2017-2018, n° 54-3126/001, p. 232. Soulignons toutefois qu'un recours devant la Cour constitutionnelle a été introduit par la Fédération des entreprises de Belgique au motif que la version actuelle de la loi ne prévoit pas de sanction administrative pour le secteur public.

95 Article 35.1 RGPD.

96 Article 35.10 RGPD.

97 La position du législateur fédéral est ainsi justifiée dans l'Exposé des motifs par le paragraphe suivant: « Lors de l'élaboration de la base légale, il est souvent difficile de voir dans les détails quels seront les mesures et mécanismes de sécurité pratiques et techniques qui seront les plus à mêmes de répondre aux risques décelés dans l'analyse. De même, lors de la mise en place du traitement, il peut s'avérer que les mesures et mécanismes mis en place génèrent des risques supplémentaires qui n'avaient pas été pris en compte de la première analyse » ; voy. projet de loi du 11 juin 2018 relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, Exposé des motifs, *Doc. parl.*, Ch. repr., 2017-2018, n° 54-3126/001, p. 49.

98 CPVP, recommandation d'initiative n° 01/2018 concernant l'analyse d'impact relative à la protection des données 01/2018 du 28 février 2018.

III. CONCLUSION

Le fonctionnement isolé des différents organismes publics a été bouleversé pour donner la place à un fonctionnement en réseau accompagné du principe de collecte unique des données à caractère personnel auprès des citoyens. La conséquence directe est une plus grande circulation des données et un accroissement des transferts de données à caractère personnel entre les différents organismes publics belges.

Pour encadrer ces échanges, le législateur fédéral a rendu obligatoire la conclusion d'un protocole entre les différentes entités concernées par le transfert. Si l'objectif poursuivi est louable, à savoir celui d'une responsabilisation accrue de tous les intervenants dans la chaîne de traitement des données à caractère personnel, il est à craindre qu'il soit amoindri par un protocole dont son contenu est rendu incertain. À l'heure actuelle, le contenu proposé fait écho aux différents principes généraux applicables à tout traitement de données à caractère personnel, à savoir les principes de loyauté et de transparence, de limitation des finalités, de minimisation des données et de sécurité, permettant dès lors aux responsables du traitement de se poser les questions adéquates pour assurer la légalité du transfert des données à caractère personnel des citoyens.

Notons que certaines recommandations de l'ancienne CPVP, appuyées par le Conseil d'État, n'ont pas été suivies lors de l'adoption de la version définitive de la loi. En effet, sont absentes du contenu proposé la description des finalités pour lesquelles les données à caractère personnel avaient été collectées à l'origine, l'analyse de compatibilité de la finalité nouvelle avec celle poursuivie à l'origine en cas de traitement ultérieur ainsi que la vérification du respect du principe de collecte auprès de la source authentique des données.

En outre, la loi clarifie les interventions du DPO et la nécessaire réalisation d'une analyse d'impact.

S'il convient de souligner les précisions apportées par la loi du 30 juillet 2018, il nous paraît qu'elles doivent s'accompagner de lignes directrices et de politiques claires et coordonnées au sein des différentes autorités publiques fédérales et, plus largement, au sein des différents niveaux de pouvoir.

Il convient également d'insister sur la plus-value pouvant être apportée par des protocoles clairs et précis et ne pas se centrer uniquement sur une potentielle charge administrative supplémentaire, au risque de perdre de vue la sécurité juridique offerte par ce protocole.