Présentation générale du R.G.P.D. et des lois belges relatives à la protection des données

De Terwangne, Cecile

Published in:
Le Règlement général sur la protection des données (R.G.P.D./G.D.P.R.)

Publication date:
2020

Document Version
le PDF de l'éditeur

1

PRÉSENTATION GÉNÉRALE DU R.G.P.D. ET DES LOIS BELGES RELATIVES À LA PROTECTION DES DONNÉES

Cécile DE TERWANGNE
professeure extraordinaire à l'UNamur (Centre de Recherche Information, Droit et Société – CRIDS)

Sommaire

Introduction

Quatre lettres, dans un sens (R.G.P.D.) ou dans un autre (G.D.P.R.), sont passées à la postérité depuis le 27 avril 2016, date de l'adoption par l'Union européenne du règlement général sur la protection des données[1]. Ce texte, entré en application le 25 mai 2018, s'accompagne en Belgique de plusieurs lois venues apporter leur lot de compléments. L'ensemble est destiné à offrir une réponse juridique actualisée aux risques et déséquilibres nés des développements techniques et des pratiques qui y sont liés. Les données à caractère personnel qui sont visées par ce régime de protection sont aujourd'hui l'objet de toutes les convoitises. Leur collecte, croisement, partage et revente sont la base d'activités économiques lucratives, de nouveaux agissements sociaux et de promesse d'efficacité administrative inégalée. Dans les mains des acteurs tant publics que privés, ces données sont aussi l'instrument d'une surveillance omniprésente : surveillance des paroles et des actes, des intérêts et des choix, des liens sociaux et des déplacements[2].

La protection des données à caractère personnel est érigée en droit fondamental depuis l'adoption du Traité de Lisbonne en décembre 2007 et figure à l'article 8 de la Charte des droits fondamentaux de l'Union européenne et à l'article 16 du Traité sur le fonctionnement de l'Union européenne. Le R.G.P.D. a donc pour vocation de mettre en œuvre la protection de ce droit fondamental[3].

Le R.G.P.D. a pris le relais de la directive européenne 95/46[4] qui avait été transposée en Belgique par la loi vie privée du 8 décembre 1992[5]. Cette loi a été abrogée le 5 septembre 2018, lors de l'entrée en vigueur de la nouvelle loi générale (ci-après, « loi-cadre ») complétant le R.G.P.D. sur les points où celui-ci a laissé une latitude aux États membres ainsi que dans les matières relevant de la directive 2016/680 « police-justice »[6], de la politique étrangère et

1 Règlement (UE) nº 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), *J.O.U.E.*, 4 mai 2016, L 119/1 (en anglais : *General Data Protection Regulation*, G.D.P.R.).

2 Voy. C. de Terwangne, « Internet et la protection de la vie privée et des données à caractère personnel », *in* Q. Van Enis et C. de Terwangne (éd.), *L'Europe des droits de l'homme à l'heure d'Internet*, Bruxelles, Larcier, 2019, pp. 325 à 368.

3 C. Ponsart et R. Robert, « Le règlement européen de protection des données personnelles », *J.T.*, 2018, p. 421.

4 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.

5 Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

6 Directive 2016/680/UE du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel 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, et à la libre circulation de ces données, et abrogeant la

de sécurité commune, ou échappant à la compétence de l'Union européenne (la sécurité nationale et la défense)[7]. L'ancien président de la Commission de la protection de la vie privée, W. Debeuckelaere, a présenté ce dernier texte sur un ton quelque peu amer : « la nouvelle loi sur la protection des données : 286 articles, quatre autorités fédérales pour la protection des données. Les choix laissés ouverts par le règlement se font toujours au détriment de la protection des données »[8]. Des 286 articles en question, on n'évoquera pas dans les pages qui suivent ceux dédiés aux traitements de données en matière de « police-justice », de la politique étrangère et de sécurité commune de l'Union européenne, et en matière de sécurité nationale. Seuls 69 articles, en lien direct avec le R.G.P.D., seront présentés avec ce dernier. Quant aux quatre autorités fédérales de contrôle évoquées par W. Debeuckelaere, seule l'autorité générale de protection des données sera retenue dans la présente analyse.

La loi-cadre du 30 juillet 2018 faisait suite à une première loi, adoptée le 3 décembre 2017 afin de transformer l'ancienne Commission de la protection de la vie privée en Autorité de protection des données (A.P.D.)[9], organe fédéral de contrôle du respect des règles de protection mises en place.

Ce dispositif général de protection est complété par des textes particuliers tels que la loi instituant le Comité de sécurité de l'information[10] qui crée un cadre pour les échanges de données des entités publiques, la loi sur le Registre national, réécrite[11] à la suite de l'adoption du R.G.P.D., ou la loi caméras elle aussi largement remaniée le 21 mars 2018[12].

décision-cadre 2008/977/JAI du Conseil. Voy. C. Forget, « La protection des données dans le secteur de la "police" et de la "justice" », *in* C. de Terwangne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, coll. du CRIDS, Bruxelles, Larcier, 2018, pp. 865 à 900.

7 Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (ci-après, « loi-cadre »).

8 Autorité de protection des données (ci-après, « A.P.D. »), « 2018 l'année du déploiement », *Rapport annuel 2018*, www.autoriteprotectiondonnees.be/jaarverslag-rapport-annuel/fr/index.html

9 Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, modifiée par la loi du 4 mars 2018 et par la loi du 25 mai 2018.

10 Loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) nº 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. Sur cette loi, voy. L. Gérard, « Le Comité de sécurité de l'information pour contrôler les données de sécurité sociale et de santé », *in* C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique – Manuel de base*, Bruxelles, Politeia, 2019, pp. 174 et s.

11 Loi du 25 novembre 2018 portant des dispositions diverses concernant le Registre national et les registres de population. Sur cette loi, voy. É. Degrave, « L'autorisation du ministre de l'Intérieur pour contrôler les données du Registre national », *in* C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique – Manuel de base*, *op. cit.*, pp. 166 et s.

12 Loi du 21 mars 2018 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière. Sur cette loi, voy. A. Michel, « Révision de la "loi caméras" : précisions ou ambiguïtés pour l'installation et l'utilisation de caméras de surveillance », *J. T.*, 2019, pp. 149 à 160.

Les pages qui suivent se focalisent sur l'ensemble des règles de protection des données découlant du R.G.P.D. complété par la loi-cadre de juillet 2018 et la loi qui a instauré l'A.P.D., sans s'étendre sur les lois particulières qui viennent d'être évoquées. La mise en application de ces textes a déjà conduit à l'adoption d'avis et de décisions, tant du Comité européen de la protection des données que de l'A.P.D. belge, qui enrichissent utilement la présente analyse.

Section 1

Notions et champ d'application

A. Notions principales

1. Notion de donnée à caractère personnel

Comme par le passé, la « donnée à caractère personnel » est définie comme toute information qui concerne une personne physique identifiée ou identifiable (appelée la « personne concernée »)[13].

La notion de donnée à caractère personnel est particulièrement large puisqu'elle englobe n'importe quel type d'informations, qu'il s'agisse d'informations privées et confidentielles, d'informations professionnelles, d'informations objectives ou subjectives, ou encore d'informations publiques, diffusées par exemple sur le Web[14] [15].

Toute forme d'information est par ailleurs couverte. Les données peuvent ainsi prendre la forme d'écrits, d'images (photos, vidéos), de sons, il peut s'agir de données de localisation, de données de comportement en ligne, de données biométriques, etc.

N'entrent dans le champ du R.G.P.D. que les données à caractère personnel concernant une personne physique vivante[16]. Un lien doit pouvoir être établi entre l'information et la personne. Ce lien peut passer par des choses qu'il est possible de relier à une personne particulière (comme des données cadastrales[17]

13 Art. 4.1 R.G.P.D. Voy. les éclaircissements apportés sur cette notion par le Groupe de l'article 29, « Avis 4/2007 sur le concept de données à caractère personnel », 20 juin 2007, WP 136. Ces éclaircissements apportés à propos de la définition de « donnée à caractère personnel » présente dans la directive 95/46 sont toujours pertinents sous le règne du R.G.P.D. qui a repris textuellement cette définition.

14 C.J.C.E., 16 décembre 2008, *Tietosuojavaltuutettu c. Satakunnan markkinapörssi oy et Satamedia oy*, C-73/07, pt 49.

15 Pour de plus amples développements sur les différents types de données couverts, voy. C. de Terwangne, « Définitions clés et champ d'application du RGPD », *in* C. de Terwangne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, *op. cit.*, pp. 71 et s.

16 Voy. cons. 27 R.G.P.D.

17 Comité sectoriel pour l'Autorité fédérale, délibération AF nº 02/2012 du 9 février 2012 concernant la demande du S.P.F. Intérieur, Direction générale Sécurité civile, d'accéder à certaines données cadastrales (Documentation patrimoniale – S.P.F. Finances) dans le cadre de la réforme des services de secours.

ou des images satellites[18]) de sorte que les données portant sur ces choses sont aussi considérées comme des données à caractère personnel.

La personne concernée par l'information doit être identifiée ou à tout le moins identifiable pour qu'on puisse parler de « données à caractère personnel ». L'identification peut se faire de manière directe ou indirecte, par référence à un identifiant, tel qu'un numéro d'identification, des données de localisation ou un identifiant en ligne (adresse I.P., p. ex.[19]), ou en faisant intervenir un ou plusieurs éléments spécifiques propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale[20]. Le considérant 26 du R.G.P.D. apporte cette précision que le ciblage (la version anglaise utilise le terme « *singling out* », soit l'individualisation ou le ciblage) peut constituer une manière d'identifier une personne physique[21]. Une personne sera identifiable dès qu'elle pourra être traitée différemment de la masse, individualisée. Un glissement s'est opéré de la notion d'identification vers un concept d'individualisation.

La Cour de justice a précisé que pour qu'une donnée puisse être qualifiée de « donnée à caractère personnel », il n'est pas requis que toutes les informations permettant d'identifier la personne concernée se trouvent entre les mains d'une seule personne[22].

Le R.G.P.D. ne couvre pas les données (rendues) anonymes mais le texte différencie ces données des données pseudonymisées[23] – ou codées – qui, quant à elles, sont couvertes par la protection comme les autres données à caractère personnel[24].

2. Notion de traitement

Autre notion essentielle intervenant dans le régime de protection, la notion de « traitement » vise les opérations appliquées aux données à caractère personnel. L'article 4.2 du R.G.P.D. définit ainsi le traitement : « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés

18 C.P.V.P., avis n° 26/2006 du 12 juillet 2006 concernant l'utilisation d'images satellites afin de dépister et de constater des infractions aux normes urbanistiques.

19 Cons. 30 R.G.P.D. Voy. F. Zuiderveen Borgesius, « The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition », *E.D.P.L.*, 2017/1, pp. 130 à 137 ; J.-Ph. Moiny, « Are Internet protocol addresses personal data? The fight against online copyright infringement », *C.L.S.R.*, 27, 2011, pp. 348 à 361.

20 Art. 4, 1°, R.G.P.D.

21 Voy. la position développée en ce sens par le Groupe de l'article 29 dans l'avis 16/2011 du 8 décembre 2011 sur le code de bonnes pratiques de l'A.E.E.P. et de l'IAB en matière de publicité comportementale en ligne (p. 8) et C. Gayrel et R. Robert, « Proposition de règlement sur la protection des données. Premiers commentaires », *J.D.E.*, 2012, p. 175.

22 C.J.U.E., 19 octobre 2016, *Breyer*, C-582/14, EU:C:2016:779, pt 43 ; C.J.U.E., 20 décembre 2017, *Novak*, C-434/16, pt 31.

23 Définies à l'article 4.5 du R.G.P.D.

24 Cons. 26 R.G.P.D.

et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».

Les opérations entrant dans la notion de traitement sont donc particulièrement variées et vont de la collecte à la destruction des données. En fait, tout ce qui peut être fait avec des données à caractère personnel, tout type d'actions ou d'utilisations des données entre dans la définition de « traitement ». Une opération isolée peut déjà constituer un traitement, mais le plus souvent il s'agira d'un ensemble d'opérations appliquées à des données. Ce qui permettra de lier ces opérations pour les considérer comme formant un seul traitement, c'est la finalité qui est poursuivie par cet ensemble d'opérations[25]. On aura, par exemple, les traitements suivants, impliquant chacun des opérations variées : les traitements « administration du personnel », « gestion des clients », « contrôle sur le lieu de travail », « lutte contre la fraude et les infractions de la clientèle », « collecte de dons », « relations publiques », « gestion du contentieux », « gestion des emprunts de bibliothèque », « octroi de crédit », « gestion du parcours scolaire », etc.

3. Notion de responsable du traitement

Aux termes de l'article 4.7 du R.G.P.D., le responsable du traitement est celui « qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ». Le Groupe de l'article 29 a considéré qu'« être responsable du traitement résulte essentiellement du fait qu'une entité a choisi de traiter des données à caractère personnel pour des finalités qui lui sont propres »[26]. Il peut s'agir d'une personne physique ou morale d'une autorité publique, d'un service ou d'un autre organisme[27].

Deux critères interviennent donc dans l'identification du responsable d'un traitement : il s'agit de déterminer « qui dispose de la maitrise (1) dans la détermination de la finalité pour laquelle les données sont traitées (raison concrète et

25 Th. Léonard et Y. Poullet, « La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 », *J.T.*, 1999, p. 379 ; C. de Terwangne et J.-M. Van Gyseghem, « Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution », *in* C. de Terwangne (éd.), *Vie privée et données à caractère personnel*, Bruxelles, Politeia, 2013.

26 Groupe de l'article 29, « Avis n° 1/2010 sur les notions de "responsable du traitement" et de "sous-traitant" », WP 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 9.

27 Art. 4.7 R.G.P.D.

opérationnelle pour laquelle les données sont traitées [...]) ainsi que (2) dans le choix des moyens utilisés pour atteindre cette finalité »[28].

Étant donné que la qualité de responsable du traitement dépend des deux critères énoncés ci-dessus, la désignation concrète des responsables de traitement découlera d'une analyse factuelle du rôle de chaque acteur pour comprendre qui a *effectivement* un pouvoir de décision sur le traitement. « Une organisation ou une personne qui n'exerce aucune influence sur la détermination de la manière dont les données sont traitées ne peut se voir conférer la qualité de responsable de traitement »[29]. En revanche, le fait de ne pas avoir techniquement accès aux données n'est pas en soi un critère suffisant pour échapper à la qualité de responsable de traitement[30]. En outre, il est admis qu'un responsable de traitement ne perde pas cette qualité s'il délègue (à son sous-traitant p. ex.) la détermination des moyens du traitement qui ne sont pas essentiels. Cette délégation ne peut porter sur la détermination des catégories de données ou de la base légale, notamment.

Une désignation erronée du responsable du traitement, c'est-à-dire qui est contredite par la situation de fait, ne lie pas le juge ni l'autorité de contrôle qui, dans une telle hypothèse, seront amenés à qualifier de responsable du traitement la personne répondant aux critères légaux.

Par ailleurs, comme auparavant, le R.G.P.D. précise que « lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre »[31].

Signalons enfin que la qualité de responsable du traitement peut être partagée. Dans le cas où différents intervenants définissent les finalités ou les moyens du traitement, on sera en présence de plusieurs coresponsables de ce traitement[32]. Il est alors question de responsables conjoints[33]. Cette responsabilité conjointe ne signifie pas nécessairement une responsabilité équivalente des

28 A.P.D., « Le point sur les notions de responsable de traitement/sous-traitant au regard du Règlement EU 2016/679 sur la protection des données à caractère personnel (RGPD) et quelques applications spécifiques aux professions libérales telles que les avocats », www.autoriteprotectiondonnees.be/analyse-juridique-RGPD.

29 A.P.D., « Le point sur les notions de responsable de traitement/sous-traitant... », *op. cit.*, p. 1.

30 C.J.U.E., 5 juin 2018, *Wirtschaftsakademie Schleswig-Holstein*, aff. C-210/16, EU:C:2018:388 ; pour un commentaire de cet arrêt, voy. S. Xeferi, « La responsabilité conjointe de l'exploitant du réseau social et de l'administrateur d'une page fan », *R.A.E.*, 2018/2, pp. 391 à 401.

31 Art. 4.7 R.G.P.D.

32 Art. 4.7 R.G.P.D. Voy. A. Delforge, « Les obligations générales du responsable du traitement et la place du sous-traitant », *in* C. de Terwangne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, *op. cit.*, pp. 381 et s.

33 Art. 26 R.G.P.D. La Cour de justice de l'Union européenne a, par exemple, considéré que l'administrateur d'une page fan était responsable conjoint de certains traitements de données avec Facebook. Voy. C.J.U.E., 5 juin 2018, *Wirtschaftsakademie Schleswig-Holstein*, préc. ; C.J.U.E., 29 juillet 2019, *Fashion ID*, aff. C- 40/17.

différents intervenants. Ceux-ci peuvent être impliqués à différents stades du traitement et selon des degrés divers[34].

4. Notion de sous-traitant

Le sous-traitant est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement »[35].

Pour être considéré comme sous-traitant, il faut traiter des données à caractère personnel pour le compte du responsable du traitement mais on ne peut pas être dans une relation hiérarchique avec celui-ci[36]. Le sous-traitant doit être une personne juridiquement distincte de l'organisation du responsable du traitement[37]. Un cas fréquent de sous-traitance est celui du fournisseur de service d'hébergement sur internet ou du fournisseur de *cloud computing*[38].

Si un sous-traitant dépasse le mandat reçu du responsable du traitement et assume de ce fait un rôle important dans la détermination des finalités pour lesquelles il va traiter les données ou des modalités essentielles du traitement des données, il acquiert alors la qualité de responsable de ce (nouveau) traitement[39].

B. Champ d'application

1. Champ d'application matériel

Le R.G.P.D. de même que la loi du 30 juillet 2018 s'appliquent à tout traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier[40]. Dès qu'il est fait recours aux technologies de l'information et de la communication (informatique, réseaux de communications – internet –, puces, géolocalisation...), les règles de protection des données sont en principe applicables.

34 C.J.U.E., 5 juin 2018, *Wirtschaftsakademie Schleswig-Holstein*, préc., pt 43. Pour les conséquences découlant du statut de responsables conjoints, voy. B. Salovic, Th. Léonard et E. Wéry, « Bouton "J'aime" de Facebook : voici le verdict final de la C.J.U.E. », 29 juillet 2019, www.droit-technologie.org/actualites/bouton-jaime-de-facebook-voici-le-verdict-final-de-la-CJUE/.

35 Art. 4.8 R.G.P.D.

36 Groupe 29, avis n° 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », préc., p. 27.

37 A.P.D., « Le point sur les notions de responsable de traitement/sous-traitant... », *op. cit.*, p. 2.

38 Voy., à ce propos, J.-M. Van Gyseghem, « *Cloud computing* et protection des données à caractère personnel : mise en ménage possible ? », *R.D.T.I.*, n° 42, pp. 35 à 50. Voy. également Groupe de l'article 29, « Avis n° 05/2012 sur l'informatique en nuage », http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_fr.pdf.

39 A.P.D., « Le point sur les notions de responsable de traitement/sous-traitant... », *op. cit.*, p. 3.

40 Art. 2, § 1er, R.G.P.D. ; art. 2 de la loi-cadre.

Et même lorsqu'aucun recours n'est fait à de telles technologies, les données à caractère personnel seront tout de même couvertes par la législation si elles figurent dans un fichier, c'est-à-dire dans un ensemble structuré de données accessibles selon des critères déterminés[41]. C'est par la structuration des données personnelles qu'il contient, permettant l'accessibilité de ces données, que le fichier se caractérise[42]. Un classement sur la base des noms des personnes, par ordre alphabétique ou sur la base de résultats, constitue un fichier. En revanche, la prise de notes sur des feuillets, la consultation de documents papier isolés ou l'envoi par courrier ordinaire de photocopies sont hors du régime de protection. On notera qu'aujourd'hui, les situations où aucun moyen automatisé n'est mobilisé pour traiter de l'information sont de plus en plus rares[43]. Rares sont donc les cas dans lesquels on recourt à la notion de fichier.

2. Champ d'application territorial

Il a déjà été relevé qu'une des caractéristiques les plus remarquables du R.G.P.D., marquant un changement substantiel par rapport à la directive 95/46, c'est l'étendue de son champ d'application territorial[44]. Ce texte, tout comme la loi-cadre de juillet 2018, réussit à toucher des acteurs situés hors de l'Union européenne, mais actifs sur le marché européen et impactant des personnes localisées dans l'Union. Le législateur européen a été « inspiré par une volonté de réagir aux collectes et traitements à grande échelle de données de résidents européens par des sociétés établies en dehors de l'Union »[45].

Le R.G.P.D. et la loi belge sont ainsi applicables :

- aux responsables de traitement ou sous-traitants qui ont un établissement en Belgique[46] : pour tous les traitements effectués dans le cadre des activités de cet établissement, que les traitements eux-mêmes aient lieu sur le territoire belge ou non ;
- aux responsables de traitement ou sous-traitants qui ne sont pas établis dans l'Union européenne : pour les traitements qui sont liés à l'offre (gratuite ou contre paiement) de biens ou de services à des personnes concernées

41 Art. 4.6 R.G.P.D.

42 C. de Terwangne, J. Herveg et J.-M. Van Gyseghem, *Le divorce et les technologies de l'information et de la communication : introduction à la protection des données dans la preuve des causes de divorce*, Kluwer, 2005, p. 12.

43 Voy. C. de Terwangne, « La difficile application de la législation de protection des données à caractère personnel : observations sous Cass. (2e ch.), 22 février 2017 », *J.T.*, 2017, pp. 752 et s.

44 C. de Terwangne, K. Rosier et B. Losdyck, « Lignes de force du nouveau règlement relatif à la protection des données à caractère personnel », *R.D.T.I.*, 2016/62, p. 14, n° 12.

45 C. de Terwangne, K. Rosier et B. Losdyck, « Lignes de force du nouveau règlement relatif à la protection des données à caractère personnel », *op. cit.*, p. 16, n° 15.

46 Voy. C. Ponsart et R. Robert, « Le règlement européen de protection des données personnelles », *op. cit.*, p. 423. Sur la notion d'établissement, voy. C.J.U.E., 13 mai 2014, *Google Spain*, C-131/12, obs. E. Defreyne et R. Robert, *R.D.T.I.*, 2014/56, pp. 53 et s. ; C.J.U.E., 1er octobre 2015, *Weltimmo*, C-230/14 ; Th. Léonard et D. Chaumont, « Données personnelles : le critère de l'installation stable est de plus en plus large », 29 octobre 2015, www.droit-technologie.org.

se trouvant sur le territoire belge, ou qui sont liés au suivi du comportement de ces personnes, si ce comportement a lieu sur le territoire belge.[47] C'est donc la localisation du public cible du traitement des données qui est le critère déterminant dans ce cas. Et l'intention de viser ce public cible peut être établie à partir d'indicateurs comme l'utilisation d'une langue ou d'une monnaie d'un État membre[48].

Les acteurs localisés hors de l'Union doivent désigner un représentant établi sur le territoire de l'Union[49], sauf si le responsable du traitement est une autorité publique ou un organisme public ou encore lorsque le traitement ne présente pas vraiment de risque[50].

La loi-cadre précise en outre que, lorsque le responsable du traitement est établi dans un État membre de l'Union européenne et fait appel à un sous-traitant établi sur le territoire belge, c'est le droit de l'État membre en question qui s'appliquera au sous-traitant et non la loi belge, pour autant que le traitement ait lieu sur le territoire de cet État membre[51]. Cette option vise à éviter les éventuels conflits de lois dans les cas où deux lois s'appliqueraient à un même traitement : la loi du responsable du traitement et la loi du sous-traitant[52].

Enfin, la loi s'applique au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi sur le territoire belge mais dans un lieu où le droit belge s'applique en vertu du droit international public[53].

47 Art. 3, § 2, R.G.P.D. Pour de plus amples développements sur ces hypothèses, voy. C. de Terwangne, « Définitions clés et champ d'application du RGPD », *in* C. de Terwangne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, *op. cit.*, pp. 75 et s. ; C. Ponsart et R. Robert, « Le règlement européen de protection des données personnelles », *op. cit.*, p. 423 ; F. Jault-Seseke, « La portée extraterritoriale ou a-territoriale du RGPD », *R.A.E./L.E.A.*, 2018/1, pp. 43 et s. Art. 4, §§ 1er et 2, de la loi-cadre.

48 En revanche, « la simple accessibilité du site internet du responsable du traitement, d'un sous-traitant ou d'un intermédiaire dans l'Union, d'une adresse électronique ou d'autres coordonnées, ou l'utilisation d'une langue généralement utilisée dans le pays tiers où le responsable du traitement est établi ne suffit pas pour établir cette intention » (cons. 23 R.G.P.D.).

49 Art. 27 R.G.P.D.

50 Art. 27, § 2, R.G.P.D. « Au grand regret d'un certain nombre d'auteurs, aucune obligation de démonstration de solvabilité n'est mise en place par le législateur européen. Amenée tant à supporter les obligations s'imposant au responsable du traitement qu'à supporter les sanctions prononcées à l'encontre du responsable, la preuve de la solvabilité du représentant aurait pourtant constitué une garantie additionnelle de la protection de la vie privée et de la mise en œuvre du futur règlement » (N. Metallinos et N. Botchorichvili, « Réforme du cadre européen de la protection des données à caractère personnel : où en est-on ? », *R.L.D.I.*, n° 99, 2013, 3303, p. 10). On craint dès lors que, malgré la volonté de donner au règlement une portée extraterritoriale, l'impact de ses dispositions ne reste que mitigé (G. Skouma et L. Léonard, « Les grands changements liés à la réglementation sur la protection des données personnelles et ses implications pratiques pour les entreprises et les professionnels », *in La protection des données en pratique*, Bruxelles, Larcier, 2016, p. 413).

51 Art. 4, § 3, de la loi-cadre.

52 Projet de loi 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. 16.

53 Art. 4, § 4, de la loi-cadre.

3. Exclusion des traitements à des fins personnelles et domestiques

Comme par le passé, les opérations effectuées sur des données à caractère personnel « par une personne physique dans le cadre d'une activité strictement personnelle ou domestique » sont exclues du champ des règles de protection des données[54].

Le considérant 18 du R.G.P.D. clarifie le fait que cette exception s'applique dans le contexte d'internet. Diffuser des données sur autrui par le biais des réseaux sociaux ou stocker des photos dans le *cloud* peut se faire sans se soumettre aux règles de protection des données à caractère personnel, pourvu toutefois qu'on veille à ce que l'on conserve à ces opérations le caractère strictement personnel. Pour cela, les données ne peuvent pas être accessibles à un nombre indéterminé de personnes, ni même à un trop grand nombre, ni enfin à des personnes qui ne présentent pas de lien (familial, affectif ou de connaissance) avec la personne qui traite les données[55].

Cette exception est bien évidemment valable hors du contexte d'internet. Elle peut s'appliquer à la caméra placée dans une maison ou dans la chambre d'un bébé, aux agendas et carnets d'adresses privés, aux listes d'amis invités pour un événement privé, etc. La Cour de justice de l'Union européenne a eu l'occasion, le 10 juillet 2018, de réaffirmer que l'exception doit être interprétée comme visant uniquement les activités qui s'insèrent dans le cadre de la vie privée ou familiale des particuliers, soit les activités qui ne dépassent pas la sphère privée[56]. L'exception ne couvre donc pas, par exemple, les traitements de données récoltées à la suite d'action de prédication de porte-à-porte (ce qui était précisément l'objet de l'affaire des Témoins de Jéhovah tranchée en 2018

54 Art. 2, § 2, c), R.G.P.D. Pour d'amples développements sur cette exception, voy. C. DE TERWANGNE, « Exclusion du champ d'application pour les traitements à des fins exclusivement personnelles ou domestiques », *in* C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique – Manuel de base*, *op. cit.*, pp. 26 et s.

55 Voy. à cet égard : C.J.U.E, 14 février 2019, *Buivids*, C-345/17, pt 43 : « Dans la mesure où M. Buivids a publié, sans restriction d'accès, la vidéo en cause sur un site internet de vidéos sur lequel les utilisateurs peuvent envoyer, regarder et partager celles-ci, rendant ainsi accessibles des données à caractère personnel à un nombre indéfini de personnes, le traitement de données à caractère personnel en cause au principal ne s'inscrit pas dans des activités exclusivement personnelles ou domestiques ». Également C.J.U.E., 11 décembre 2014, *František Ryneš c. Úřad pro ochranu osobních údajů*, aff. C-212/13 ; C.J.C.E., 16 décembre 2008, *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy, Satamedia Oy*, aff. C73/07, pt 44 ; C.J.C.E., 6 novembre 2003, *Lindqvist*, aff. C-101/01, pt 47 ; C. DE TERWANGNE, « L'exception concernant les traitements de données à des fins personnelles et domestiques de la Directive 95/46/CE relative à la protection des données : note sous Cour de justice de l'Union européenne, 11 décembre 2014 », *R.D.T.I.*, 2015, n° 58, pp. 39 à 51 ; Groupe de l'article 29, Statement of the Working Party on current discussions regarding the data protection reform package. Annex 2: Proposals for Amendments regarding exemption for personal or household activities, 27 février 2013, http://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf, p. 4.

56 C.J.U.E. (Gde ch.), 10 juillet 2018, *Jehovan todistajat*, aff. C-25/17.

par la Cour de justice), ni les captures d'images faites par un drone dans l'espace public, ou par une caméra débordant partiellement sur la voie publique[57].

4. Régime dérogatoire pour les traitements à des fins journalistiques ou d'expression universitaire, artistique ou littéraire

Les traitements effectués aux seules[58] fins de journalisme ou d'expression universitaire, artistique ou littéraire bénéficient d'un régime d'exceptions partielles aux règles de protection des données. Une série de dispositions peuvent ne pas être appliquées à ces traitements, afin de garantir un équilibre avec la protection de la liberté d'expression[59]. Cet équilibre étant fonction de divergences culturelles, le législateur européen s'en est remis à chaque législateur national pour effectuer la pondération entre les droits fondamentaux concurrents et déterminer le point d'équilibre[60].

Il s'ensuit qu'il n'y a pas d'homogénéité en la matière sur le continent européen. Selon le considérant 153, « [l]orsque ces exemptions ou dérogations diffèrent d'un État membre à l'autre, le droit de l'État membre dont relève le responsable du traitement devrait s'appliquer ».

Les personnes s'adonnant à des activités journalistiques ou exerçant leur expression académique, artistique ou littéraire sont incluses dans le champ de la législation (R.G.P.D. et loi-cadre), mais elles bénéficient d'un allégement de certaines règles. Il s'agit des règles dont l'application mettrait en péril la correcte réalisation des finalités en question. L'article 85 s'inscrit dans la ligne de l'article 9 de la directive 95/46 et permet aux États de prévoir un très large régime d'exception puisque ce régime peut déroger à l'ensemble des principes de protection, aux droits des personnes concernées, aux obligations du responsable du traitement, au régime des flux transfrontières de données, aux pouvoirs des autorités de contrôle et aux régimes spécifiques. La seule limite est que seules les exceptions véritablement nécessaires pour concilier le droit à la protection des données à caractère personnel et la liberté d'expression et d'information

57 C.J.U.E., 11 décembre 2014, *Frantisek Ryneš*, aff. C-212/13.

58 Si le texte de l'article 85 dit « aux fins », le considérant 153 qui l'éclaire énonce : « Dans le cadre du traitement de données à caractère personnel *uniquement* à des fins journalistiques ou à des fins d'expression universitaire, artistique ou littéraire, il y a lieu de prévoir des dérogations [...] » (nos italiques). Sur ce point, voy. Q. VAN ENIS, « La conciliation entre le droit à la liberté d'expression et le droit à la protection des données à caractère personnel dans le R.GPD », *in* C. de Terwangne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, *op. cit.*, pp. 782 et s.

59 Art. 85, § 1er, R.G.P.D.

60 Quentin Van Enis déplore cette « abdication » du législateur européen et que ce dernier ne soit pas allé plus loin dans la recherche d'un plus petit dénominateur commun entre les différents États membres. « L'article 85 se révèle évasif et à peine plus loquace que la directive qu'il remplace sur la manière dont la protection des données et la liberté d'expression seront amenées à coexister paisiblement à partir du 25 mai 2018 » (Q. VAN ENIS, « La conciliation entre le droit à la liberté d'expression et le droit à la protection des données à caractère personnel dans le R.G.P.D. », *op. cit.*, pp. 766 et 767 et pp. 785 et s., nos 17 et s., spéc. n° 20).

sont admises[61]. L'article 24 de la loi-cadre contient les exemptions admises par le législateur belge qui s'est montré étonnamment plus laxiste que par le passé, dispensant d'office de l'application des règles concernant le consentement, les données sensibles et tous les droits des personnes concernées. De façon plus respectueuse de l'article 85 du R.G.P.D., les autres dérogations (prévues aux paragraphes 3 à 5 de l'article 24 de la loi-cadre) ne sont admises que dans des circonstances spécifiques, lorsque cela s'impose pour la conciliation des droits concurrents[62].

Section 2
Principes relatifs au traitement des données à caractère personnel

L'article 5 du R.G.P.D. énonce l'ensemble des principes de base de la protection des données. Ces principes sont présentés dans les paragraphes qui suivent mais, auparavant, il convient de mettre en exergue une exigence qui n'est pas énoncée textuellement dans cet article mais qui est formulée tant dans la jurisprudence[63] que dans les travaux préparatoires de la loi-cadre[64] et à l'article 5, § 1er, de la Convention nº 108 modernisée du Conseil de l'Europe[65] en voie de ratification par la Belgique : le respect du principe de proportionnalité.

A. Principe de proportionnalité

Tout traitement des données doit présenter un caractère proportionné, c'est-à-dire respecter un juste rapport de proportionnalité entre les moyens utilisés et le but à atteindre. Pour cela, il doit être pertinent au regard de la finalité légitime poursuivie, et être limité à ce qui est nécessaire au regard des intérêts, droits et libertés des personnes concernées ou de l'intérêt public. Il ne doit pas induire une ingérence disproportionnée dans ces intérêts, droits et libertés. Le principe de proportionnalité doit être respecté à toutes les étapes du traitement,

61 Art. 85, § 2, *in fine*, R.G.P.D.

62 Pour une présentation détaillée du régime dérogatoire réservé aux traitements à des fins journalistiques ou d'expression universitaire, artistique ou littéraire, voy. C. de Terwangne, « Les traitements à des fins journalistiques ou d'expression universitaire, artistique ou littéraire », *in* C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique – Manuel de base*, *op. cit.*, pp. 115 et s.

63 C.J.U.E. (Gde ch.), 9 novembre 2010, *Volker und Markus Schecke et Eifert*, aff. jointes C-92/09 et C-93/09, pt 77 ; (Gde ch.), 8 avril 2014, *Digital Rights Ireland e.a.*, aff. jointes C-293/12 et C-594/12, pt 52 ; (Gde ch.), 6 octobre 2015, *Schrems*, aff. C-362/14, pt 92 ; (Gde ch.), 19 décembre 2016, *Tele2 Sverige*, aff. jointes C-203/15 et 698/15, pts 94 et s. ; Cour eur. D.H. (Gde ch.), *S. et Marper c. Royaume-Uni*, 4 décembre 2008, req. nos 30562/04 et 30566/04, § 118.

64 Projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, avis du Conseil d'État, *Doc. parl.*, Ch. repr., 2017-2018, nº 54-3126/1, pp. 406 et 407.

65 Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (S.T.E. nº 108), 10 octobre 2018, art. 5, § 1er.

à commencer par le stade initial, c'est-à-dire lorsqu'il est décidé de procéder au traitement des données[66].

Il faut donc mettre en balance l'ensemble des intérêts, droits et libertés en jeu avant le lancement de tout traitement de données, et les opérations ne peuvent être faites sur des données que si le résultat de la mise en balance est équilibré. Et cela, même si on a obtenu le consentement des personnes concernées ou si on s'appuie sur une autre base légale. Un traitement de données pourrait ainsi être condamné par un juge ou par une autorité de contrôle s'il ne répond pas à l'exigence de proportionnalité, malgré le fait que les personnes concernées aient consenti à ce traitement. Outre les problèmes fréquents de qualité des consentements, il se peut en effet que ce qu'une personne est prête à accepter pour son intérêt particulier (attirée par la facilité – le recours à la reconnaissance faciale p. ex. – ou par un avantage financier) ne soit pas tolérable pour l'ensemble de la société (mise en place insidieuse d'une société de surveillance p. ex.).

B. Principe de licéité

Les données à caractère personnel doivent être traitées de manière licite[67]. Cette exigence de licéité signifie que le traitement de données à caractère personnel doit se faire conformément à l'ensemble des règles légales applicables. Cela implique le respect des règles de protection des données, mais également de toute autre exigence légale qui trouverait à s'appliquer à une situation de traitement de données, comme les obligations en matière de droit du travail ou de protection du consommateur, ou le respect de l'exigence de légalité découlant de l'article 22 de la Constitution et imposant d'encadrer par une loi tout dispositif portant atteinte au droit à la vie privée[68].

C. Principe de loyauté et transparence

L'exigence de loyauté[69] induit que le traitement des données soit réalisé dans la transparence pour les personnes concernées, et sans tromperie[70]. Les traitements de données ne peuvent se faire à l'insu des personnes sur qui portent les données, d'une manière qui serait tout à fait inattendue ou imprévisible pour elles.

66 Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (S.T.E. nº 108), Rapport explicatif, 18 mai 2018, § 40.

67 Art. 5, § 1er, a), R.G.P.D.

68 Sur cette exigence de légalité, et notamment les éléments que doit contenir la loi en question, voy. É. Degrave, *L'e-gouvernement et la protection de la vie privée*, coll. du CRIDS, Bruxelles, Larcier, 2014.

69 Sur ce principe, voy. not. F. Dumortier, C. Gayrel, J. Jouret, D. Moreau et Y. Poullet, « La protection des données dans l'Espace européen de liberté, de sécurité et de justice », *J.D.E.*, 2010, p. 35.

70 Art. 5, § 1er, a), R.G.P.D.

Dans un souci de clarté, les auteurs du R.G.P.D. ont souhaité faire figurer explicitement le principe de transparence aux côtés de l'exigence de traitement loyal, étant donné le lien existant entre ces deux principes[71]. L'exigence de transparence fait par ailleurs l'objet de dispositions spécifiques consacrées au devoir d'information pesant sur le responsable du traitement : les articles 12 à 14 du R.G.P.D.[72].

D. Principe de limitation des finalités

Véritable pierre angulaire de la protection des données, le « principe de finalité », tel qu'il est couramment nommé, exige que les données soient collectées pour des finalités déterminées, explicites et légitimes, et ne soient pas traitées ultérieurement de manière incompatible avec ces finalités[73]. Les finalités du traitement des données doivent donc être fixées et claires dès le début[74]. Pour être légitimes, elles ne peuvent induire une atteinte disproportionnée aux droits, libertés et intérêts en jeu, au nom des intérêts poursuivis par le responsable du traitement[75]. La notion de finalité légitime renvoie « à des principes de droit plus généraux, tels que le principe de non-discrimination »[76].

On peut effectuer sur ces données toutes les opérations qui seront considérées comme compatibles avec les finalités d'origine, c'est-à-dire qui entrent dans les attentes raisonnables des intéressés du fait du lien qu'elles présentent avec la finalité initiale ou du contexte[77]. L'A.P.D. le dit dans ces termes : « une finalité compatible est par exemple une finalité que la personne concernée peut prévoir ou qui peut être considérée comme compatible en vertu d'une disposition légale »[78]. Cette autorité a eu à connaître de plusieurs cas de réutilisation de données dans le cadre de la campagne électorale du printemps 2019. Elle a condamné d'une amende de 5.000 euros ces réutilisations qui se faisaient à

71 C. Ponsart et R. Robert, « Le règlement européen de protection des données personnelles », *op. cit.*, p. 423.

72 Voy. *infra*, section 6.

73 Art. 5, § 1er, b), R.G.P.D.

74 Pour un cas où l'A.P.D. a recommandé de définir plus clairement et explicitement dans un arrêté du gouvernement flamand les finalités des communications de données envisagées, voy. A.P.D., avis n° 83/2018 du 5 septembre 2018 concernant un avant-projet de décret relatif à la délinquance environnementale, pts 4 et 5.

75 M.-H. Boulanger, C. de Terwangne, Th. Léonard, S. Louveaux, D. Moreau et Y. Poullet, « La protection des données à caractère personnel en droit communautaire », *J.T.-dr. eur.*, 1997, p. 145 ; Th. Léonard et Y. Poullet, « Les libertés comme fondement de la protection des données nominatives », *in* F. Rigaux (dir.), *La vie privée : une liberté parmi les autres ?*, Bruxelles, Larcier, 1992, pp. 231 et s.

76 C. Ponsart et R. Robert, « Le règlement européen de protection des données personnelles », *op. cit.*, p. 423. Également Groupe de l'article 29, « Opinion 03/2013 on purpose limitation », 2 avril 2013, WP 203, p. 12.

77 Voy. art. 6, § 4, et cons. 50 R.G.P.D.

78 A.P.D. (ch. contentieuse), décision 11/2019 du 25 novembre 2019, p. 6.

l'encontre du principe de finalité[79]. Pour établir le montant de cette amende, elle a tenu compte de la nature de la violation, du caractère intentionnel, de la finalité du traitement (influencer le choix électoral), de la qualité des intervenants (mandataires publics élus), et du nombre de personnes concernées par le traitement[80].

Il est permis dans deux cas de traiter des données à une fin différente de celle pour laquelle elles ont été collectées, sans s'interroger sur la compatibilité de cette nouvelle finalité avec la première : avec le consentement de la personne concernée pour ce traitement ultérieur ou lorsque celui-ci est fondé sur le droit de l'Union ou le droit national.

Enfin, on signalera que certaines réutilisations des données sont considérées comme compatibles moyennant certaines conditions[81]. Il s'agit des traitements ultérieurs « à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques »[82].

E. Principe de minimisation des données

Aux termes de l'article 5, § 1er, c), les données à caractère personnel faisant l'objet d'un traitement doivent être adéquates et pertinentes au regard des finalités du traitement. Elles doivent en outre être « limitées à ce qui est nécessaire », ce qui doit se comprendre en termes quantitatifs (pas trop de données) et qualitatifs (pas de données qui portent excessivement atteinte à la personne concernée). Le principe de minimisation des données conduit à ce que l'on ne puisse traiter des données à caractère personnel que lorsqu'il n'y a pas raisonnablement moyen d'atteindre la finalité sans cela[83]. Il est précisé au considérant 39 que cela implique en outre que la durée de conservation des données soit limitée « au strict minimum ».

79 *Ibid.* Voy. également A.P.D. (ch. contentieuse), décision 4/2019 du 28 mai 2019, www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/BETG04-2019ANO_FR.pdf et décision 10/2019 du 25 novembre 2019, www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/DEDF10-2019_FR.pdf.

80 *Ibid.* Th. Espeel, « RGPD et finalité du traitement : l'APD serre la vis ! », 10 décembre 2019, https://lexing.be.

81 Ces conditions sont développées à l'article 89, § 1er, du R.G.P.D., et, à sa suite, au titre 4 de la loi-cadre.

82 Art. 5, § 1er, b), *in fine*, R.G.P.D. Le régime spécifique du titre 4 de la loi-cadre réservé aux données traitées à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ne sera pas développé dans la présente contribution. Pour sa présentation voy. Th. Léonard, B. Salovic et O. Guerguinov, « R.G.P.D. et recherche scientifique : le cadre juridique en Belgique », 1er avril 2019, www.droit-technologie.org/dossiers/RGPD-et-recherche-scientifique-le-cadre-juridique-en-belgique/ ; A. Delforge, « Le régime dérogatoire pour les traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques visées à l'article 89 du RGPD », *in* C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique – Manuel de base*, *op. cit.*, pp. 124 et s.

83 Cons. 39 R.G.P.D.

Dans une affaire mettant en cause l'utilisation de la carte d'identité électronique comme carte de fidélité, l'A.P.D. a sanctionné pour recueil de données non pertinentes et violation du principe de minimisation le commerçant qui recueillait le numéro du Registre national ou une partie du numéro de la carte d'identité pour identifier ses clients, de même que leur date de naissance[84].

F. Principe d'exactitude

Les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour. Toute inexactitude doit être corrigée, l'article 5, § 1er, d, du R.G.P.D. apportant cette précision que la rectification doit être faite « sans tarder ». Il s'agit d'une « obligation de moyens en vertu de laquelle le responsable du traitement doit mettre en œuvre des mesures raisonnables afin de tenir à jour les données qu'il traite »[85], alors qu'apporter une correction en réponse à une demande de rectification formulée par la personne concernée correspond à « une obligation de résultat »[86].

G. Principe de limitation de la conservation

Il est interdit de conserver les données à caractère personnel sous une forme permettant l'identification des personnes au-delà du temps nécessaire à l'accomplissement des finalités liées au traitement de ces données. Le considérant 39 du R.G.P.D. suggère que des délais soient fixés par le responsable du traitement pour l'effacement des données ou pour une vérification périodique, afin de garantir que la conservation des données ne dépasse pas ce qui est nécessaire.

H. Principe d'intégrité et confidentialité

Sous l'intitulé d'« intégrité et confidentialité », c'est le devoir classique mais crucial de sécurité des données qui figure désormais au rang des principes de base. Les données à caractère personnel doivent être traitées de façon à leur garantir une sécurité appropriée, ce qui inclut la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle[87]. Cette protection implique de prendre les mesures techniques ou

84 La chambre contentieuse de l'A.P.D. a infligé une amende de 10.000 euros au commerçant fautif (A.P.D. (ch. contentieuse), décision 06/2019 du 17 septembre 2019, www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/BETG06_2019ANO_fr.pdf).

85 C. Ponsart et R. Robert, « Le règlement européen de protection des données personnelles », *op. cit.*, p. 424.

86 *Ibid.*

87 Art. 5, § 1er, f), R.G.P.D.

organisationnelles appropriées[88] [89]. Une section entière du chapitre dédié aux responsable et sous-traitant[90] développe ce devoir de sécurité en apportant la nouveauté de l'obligation de notifier à l'autorité de contrôle, voire aux personnes concernées, les violations de données.

Une affaire jugée le 23 janvier 2019 par le président du tribunal civil francophone de Bruxelles[91] réussit à violer tous les principes qui viennent d'être cités… Cette affaire concernait la mise en ligne sur le site jechoisismonavocat.be, par une entreprise de droit américain, d'un annuaire répertoriant tous les avocats inscrits à l'O.B.F.G., à l'insu de ceux-ci. Ce site contenait des données non fiables, fausses ou incomplètes. Le président du tribunal a condamné sous astreinte l'entreprise en question à détruire toutes les données relatives au demandeur.

I. Principe de responsabilité (*accountability*)

La liste des principes de base de la protection des données se termine par l'affirmation que revient au responsable du traitement la responsabilité du respect de tous ces principes et, nouveauté, que le responsable doit être à même de démontrer que son traitement est en conformité avec ces principes[92].

Section 3
Hypothèses de licéité des traitements de données

Les principes de protection développés dans la section qui précède sont complétés par l'exigence que chaque traitement repose sur une des bases de licéité figurant dans la liste de l'article 6, § 1er, du R.G.P.D.

88 *Ibid.*

89 Pour de très amples développements sur le principe d'intégrité et de confidentialité et l'obligation de sécurité correspondante (énoncée à l'article 32 du R.G.P.D.), voy. l'analyse très fouillée réalisée par Franck Dumortier (F. Dumortier, « La sécurité des traitements de données, les analyses d'impact et les violations de données », *in* C. de Terwangne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, *op. cit.*, pp. 143 à 253).

90 Section 2 du chapitre IV consacré aux devoirs des responsable et sous-traitant, art. 32 à 34 R.G.P.D.

91 Civ. fr. Bruxelles (prés.), 23 janvier 2019, *J.L.M.B.*, 2019/9, pp. 427 à 431.

92 Voy. également art. 24 R.G.P.D. Sur le principe d'*accountability*, voy. A. Delforge, « § 1. L'obligation générale d'"*accountability*" », *in* C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique – Manuel de base*, Bruxelles, Politeia, 2019, p. 79 ; Groupe de l'article 29, « Avis n° 3/2010 sur le principe de la responsabilité », 13 juillet 2010, WP 173.

A. Le consentement

La première hypothèse dans laquelle on peut traiter des données à caractère personnel est celle où l'on a obtenu le consentement des personnes concernées pour ce faire.

Aux termes de l'article 4, 11°, du R.G.P.D., il faut entendre par « consentement » de la personne concernée « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

Le législateur européen a voulu réagir à la multiplication des situations dans lesquelles un consentement de (très) mauvaise qualité servait de base de licéité au traitement des données. En renforçant les exigences relatives au consentement[93], il a veillé à ce que, désormais, soit le responsable du traitement s'appuie sur un consentement de bonne qualité, soit il utilise une autre base de licéité pour traiter ces données.

Pour être valide, le consentement doit donc être :

- *libre*, c'est-à-dire émis sans pression ; le consentement sera considéré comme ayant été librement donné uniquement si la personne concernée dispose d'une véritable liberté de choix ou est en mesure de refuser ou de retirer son consentement sans subir de préjudice[94]. Pour la chambre contentieuse de l'A.P.D., dans l'affaire relative à l'usage de la carte d'identité électronique comme carte de fidélité dans un commerce, le consentement ne peut pas être considéré comme libre, « faute d'un système alternatif permettant la création d'une carte de fidélité sans utilisation de la carte d'identité électronique, donnant également la possibilité dans ce cas à la personne concernée de bénéficier de réductions »[95]. « Si le consentement est présenté comme une partie non négociable des conditions générales, l'on considère qu'il n'a pas été donné librement »[96].
  En outre, le consentement ne sera pas admis comme libre lorsque l'exécution d'un contrat est suspendue au consentement pour le traitement de données qui ne sont pas nécessaires à ce contrat[97].
  De même, le consentement est présumé ne pas être libre en matière d'emploi et dans les rapports avec des autorités publiques, vu le déséquilibre existant entre les parties[98] ;

93 Les exigences supplémentaires sur ce point s'inspirent des recommandations émises par le Groupe de l'article 29 dans l'avis n° 15/2011 sur la définition du consentement, 13 juillet 2011, WP 187.

94 Cons. 42 R.G.P.D. Voy. également Groupe de l'article 29, « Guidelines on consent under Regulation 2016/679 », préc., p. 3.

95 A.P.D. (ch. contentieuse), décision 06/2019 du 17 septembre 2019, préc., p. 7.

96 *Ibid.*

97 Art. 7, § 4, et cons. 43 R.G.P.D.

98 Cons. 43 R.G.P.D. Voy. A.P.D., « Avis n° 87/2018 concernant un projet d'arrêté du gouvernement flamand relatif à l'obtention d'un titre de compétence professionnelle », 26 septembre 2018, pt 12.

- *spécifique* : le consentement ne peut être général, il doit porter sur un traitement de données précis ; si le traitement poursuit plusieurs finalités, il doit être possible de consentir à certaines finalités et pas à d'autres[99] ;
- *éclairé* : la personne concernée a reçu toute l'information utile sur le traitement envisagé ; elle doit notamment savoir qui utilisera ses données et pourquoi, et se rendre compte des destinataires de ses données ;
- *non équivoque* : le consentement doit être indiscutable, il ne peut être douteux ou ambigu ;
- enfin, le consentement doit manifester la volonté de la personne concernée *par une déclaration ou un acte positif clair* de sa part. Le silence, l'inaction et des cases cochées par défaut ne peuvent constituer un consentement[100]. Il ne peut y avoir de consentement implicite.

Au demeurant, l'article 7, § 1er, du R.G.P.D. qui est consacré aux conditions applicables au consentement impose au responsable du traitement d'être en mesure de démontrer que la personne concernée a donné son consentement au traitement de ses données. La fourniture d'une telle preuve est essentiellement envisageable en présence d'un consentement explicite. Le responsable du traitement qui fonde l'enregistrement et l'utilisation des données sur le consentement des personnes concernées doit donc veiller à conserver les traces des consentements recueillis[101].

Le R.G.P.D. stipule que la personne dont les données sont traitées doit pouvoir à tout moment retirer son consentement aussi simplement qu'elle l'a donné[102].

Une protection spécifique s'applique pour les enfants lors de l'utilisation de services de la société de l'information[103] (tels les réseaux sociaux ou les sites de jeu ou de vente en ligne) proposés directement à un enfant[104]. Le législateur belge a utilisé la latitude qui lui était laissée par le R.G.P.D. de fixer plus bas que 16 ans l'âge à partir duquel un mineur peut consentir seul au traitement de ses données lié à un service de la société de l'information. Il a établi que « le traitement des données à caractère personnel relatif aux enfants en ce qui concerne l'offre directe de services de la société de l'information aux enfants, est licite lorsque le consentement a été donné par des enfants âgés de 13 ans ou plus »[105]. Pour des données relatives à des enfants de moins de 13 ans, le traite-

99 Cons. 32 R.G.P.D. La version néerlandaise du considérant 32 du R.G.P.D. indique clairement que c'est bien pour chacune des finalités qu'il faut obtenir des personnes concernées leur consentement : « *Indien de verwerking meerdere doeleinden heeft, moet toestemming voor elk daarvan worden verleend* ».

100 *Ibid.*

101 Pour davantage de précisions sur le recueil du consentement au sein d'un contrat, voy. C. DE TERWANGNE et É. DEGRAVE, *La protection des données à caractère personnel en Belgique – Manuel de base*, *op. cit.*, p. 44.

102 Art. 7, § 3, R.G.P.D.

103 Voy. la définition du « service de la société de l'information » (art. I.18.1° C.D.E.) : « tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire du service ».

104 Art. 8, § 1er, et cons. 38 R.G.P.D.

105 Art. 7 de la loi-cadre.

ment ne sera licite que si le consentement est donné « par le représentant légal de cet enfant »[106]. Le consentement du titulaire de la responsabilité parentale n'est toutefois pas requis dans le cadre de services de prévention ou de conseil proposés directement à un enfant[107] [108].

B. Le contrat

Un traitement de données sera également licite s'il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou de mesures précontractuelles prises à la demande de celle-ci[109].

C. La sauvegarde d'un intérêt vital

Les traitements sont aussi admis lorsqu'ils sont effectués pour sauvegarder l'intérêt vital de la personne concernée, voire d'une autre personne physique. Le considérant 46 offre un exemple de situation où le traitement de données à caractère personnel est justifié par la sauvegarde d'intérêts vitaux : lorsqu'il est nécessaire à des fins humanitaires, par exemple pour suivre la propagation d'épidémies ou dans le cas de catastrophes naturelles.

D. L'obligation légale

Le traitement est également considéré comme licite lorsqu'il est « nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis »[110]. La plupart des traitements effectués par les entités du secteur public entrent dans cette hypothèse de licéité. Des obligations légales de traitements (enregistrement, communication de données…) peuvent aussi peser sur des acteurs privés, comme les employeurs, les banquiers, les assureurs, les écoles, etc. à des fins fiscales et de sécurité sociale, de lutte contre le blanchiment ou le surendettement, d'octroi de subventions…

Pour être retenue comme justifiant des traitements de données, la base légale doit répondre aux exigences que la Cour européenne des droits de l'homme a fait découler de l'article 8 de la C.E.D.H. : la norme doit être accessible et prévisible. Rappelons que, pour être prévisible, une norme doit être suffisamment détaillée pour qu'à sa lecture – en s'entourant au besoin de conseils éclairés –, on soit à même d'envisager les atteintes basées sur l'article 8, § 2, de la C.E.D.H.[111], ce qui signifie dans le cas présent qu'on se rende compte des traitements de données qui auront lieu. Dans son avis n° 56/2018 du 4 juillet 2018[112], l'Autorité de protection des données a précisé : « Les exigences en matière de vie privée de "nécessité au sein d'une société démocratique" et de "prévisibilité" de la base légale au sens des articles 8 de la C.E.D.H. et 22 de la Constitution ne sont pas respectées si le législateur n'a pas défini les éléments essentiels des traitements. […] Sur la base de la jurisprudence de la Cour européenne des droits de l'homme et de la Cour constitutionnelle ainsi que des avis antérieurs de la Commission de la protection de la vie privée, prédécesseur en droit de l'Autorité, il s'agit notamment : (1) des catégories de données traitées, (2) des parties qui auront accès aux données, (3) des finalités pour lesquelles les données pourraient être utilisées et (4) des garanties suffisantes contre les abus, dont la réglementation en matière de conservation des données »[113].

La Cour constitutionnelle a insisté que si toute personne doit avoir une idée suffisamment claire des données traitées, des personnes concernées par ce traitement de données et des conditions et finalités dudit traitement, « 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 »[114]. Le détournement de finalité, qui sort l'utilisation des données des attentes raisonnables des personnes concernées, doit être scrupuleusement compensé par une norme éclairante sur laquelle il se base.

Enfin, la Cour constitutionnelle a affirmé que, au-delà de l'exigence de qualité de la base légale, « 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 »[115].

106 Art. 7 de la loi-cadre. Les travaux préparatoires renvoient à la notion d'autorité parentale visée dans les articles 371 et suivants du Code civil et à la tutelle visée aux articles 389 et suivants du Code civil (projet de loi 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. 19).

107 Cons. 38 R.G.P.D.

108 Pour de plus amples développements sur le consentement des mineurs, voy. C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique – Manuel de base*, *op. cit.*, p. 45.

109 Art. 6, § 1er, b), R.G.P.D.

110 Art. 6, § 1er, c), R.G.P.D.

111 S.L.C.E., avis n° 63.192/2 du 19 avril 2018 sur un 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. 406.

112 A.P.D., avis n° 56/2018 du 4 juillet 2018 sur le projet de loi transposant la directive (UE) 2016/97 du Parlement européen et du Conseil du 20 janvier 2016 sur la distribution d'assurances.

113 *Ibid.*, p. 6.

114 C.C., arrêt n° 29/2018 du 15 mars 2018, B.18.

115 C.C., préc., B.14.1. Voy. spécialement les éléments à prendre en compte pour vérifier le juste équilibre.

E. La mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement

L'article 6, § 1er, e), du R.G.P.D. prévoit que sont licites les traitements 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 ».

Les finalités des traitements en cause doivent être liées à la mission d'intérêt public ou à l'exercice de l'autorité publique[116]. C'est le cas, par exemple, des traitements nécessaires à la réalisation de statistiques par l'I.N.S. ou de bases de données géographiques par l'I.G.N., ou pour la gestion des abonnements des transports en commun, etc.

Ici tout comme dans les cas précédents, il faut vérifier si les opérations effectuées sur les données (enregistrement, utilisation, transfert…) sont véritablement nécessaires pour exécuter la mission d'intérêt public ou relevant de l'exercice de l'autorité publique[117].

F. Les intérêts légitimes du responsable du traitement ou d'un tiers

Dernière hypothèse de licéité, le traitement de données est admis s'il est nécessaire « aux fins des intérêts légitimes »[118] du responsable du traitement ou d'un tiers, « à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant »[119]. Cette base légale est en fait une base « fourre-tout » destinée à permettre des traitements qui doivent être considérés comme admissibles, car légitimes, mais qui ne correspondent à aucune des autres hypothèses de la liste de l'article 6 du R.G.P.D. Aux termes des considérants 47 et 49 du R.G.P.D., les traitements à des fins de prévention de la fraude ou à des fins de prospection commerciale ou ceux visant à garantir la sécurité du réseau et des informations peuvent licitement se fonder sur une hypothèse de balance d'intérêts.

L'attention apportée à la fin de la disposition aux enfants (« notamment lorsque la personne concernée est un enfant ») invite à tenir particulièrement

116 Art. 6, § 3, al. 2, R.G.P.D.

117 Voy. E.D.P.S., *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, 11 avril 2017, https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_fr.pdf.

118 Le texte anglais du règlement est resté le même que celui de la directive sur ce point, mais la traduction française a, elle, varié. On est passé de la formulation « nécessaire à la réalisation des intérêts légitimes […] » à une formulation moins heureuse « nécessaire aux fins des intérêts légitimes […] ».

119 Art. 6, § 1er, f), R.G.P.D.

compte, lors de la mise en balance, de l'éventuelle qualité d'enfant de la personne concernée.

Enfin, on signalera que les auteurs du R.G.P.D. excluent expressément de cette hypothèse de licéité les traitements effectués par les autorités publiques dans l'exécution de leurs missions[120]. Pour ces traitements, l'exigence de légalité impose au législateur de prévoir par la loi la base juridique justifiant le traitement des données à caractère personnel par les autorités publiques[121].

Section 4

Traitement des catégories particulières de données

A. Les données sensibles

L'identification d'une catégorie particulière de données à caractère personnel, appelées couramment les « données sensibles », auxquelles on réserve une protection plus élevée est liée aux risques accrus de porter préjudice aux individus sur la base du traitement de ces données. C'est principalement le risque de discriminations illégitimes ou arbitraires qui est lié à ces données qui justifie le traitement différencié qui leur est accordé[122]. De telles données présentent, en outre, un risque d'affecter la sphère la plus intime des sujets de données ainsi qu'un risque sérieux de dommage, en cas d'abus, pour la personne concernée.

Les données sensibles sont, selon la liste de l'article 9, § 1er, du R.G.P.D. les données qui révèlent l'origine raciale et ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale et les données concernant la santé et la vie sexuelle, l'orientation sexuelle, les données génétiques et les données biométriques traitées aux fins d'identifier une personne physique de manière unique[123].

Le contexte dans lequel ces données sont traitées peut engendrer des risques pour les droits et libertés[124]. L'impact du contexte sur le caractère sensible d'une donnée est surtout important en présence de données qui ne seront pas dans tous les cas à considérer comme sensibles. C'est le cas, par exemple de la photo d'un individu. Elle révèle son origine raciale ou ethnique mais ce ne sera très souvent pas cet aspect-là qui sera traité lors de l'enregistrement et de l'utilisation de la photographie. Ce ne sera donc que dans le cas où le traitement de photos est réalisé afin d'établir l'origine raciale ou ethnique des individus apparaissant sur les clichés que les photos devront être considérées comme des

120 Art. 6, § 1er, al. 2, R.G.P.D.

121 Cons. 47.

122 Voy. J. Ringelheim, « Recueil des données personnelles et lutte contre les discriminations. Une tension nécessaire entre non-discrimination et vie privée », *in Les nouvelles lois luttant contre la discrimination*, Bruges, la Charte, 2008, pp. 91 et s.

123 Art. 9, § 1er, R.G.P.D.

124 Cons. 51 R.G.P.D.

données sensibles et seront protégées par le régime plus strict accordé à de telles données. Le considérant 51 apporte un autre exemple de l'impact du contexte de traitement sur la notion de données sensibles. Il s'agit encore du traitement de photographies mais cette fois pour en extraire des données biométriques. D'après le considérant, il ne faut pas faire systématiquement entrer toute photographie dans la définition de données biométriques. Ce ne sera que «lorsqu'elles sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique», comme dans le cas de badges utilisés pour accéder à des locaux, que les photos correspondront à des données biométriques et bénéficieront du régime restrictif des données sensibles.

Un régime plus protecteur que pour les données ordinaires est réservé à ces données. C'est le principe d'interdiction de traitement qui prévaut, assorti d'exceptions pour lesquelles leur traitement est admis moyennant le plus souvent des garanties additionnelles telles que l'adoption d'une norme qui prévoit des garanties appropriées[125]. Parmi ces exceptions figurent les hypothèses où la personne concernée a donné son consentement explicite, où le traitement est imposé par le droit du travail ou de la sécurité sociale, où le traitement est nécessaire pour la défense d'un droit en justice, ou pour l'octroi de soins médicaux[126].

Une de ces exceptions permet les traitements nécessaires pour des motifs d'intérêt public important sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée[127]. La Belgique a donc saisi cette marge de manœuvre laissée par le législateur européen. L'article 8 de la loi-cadre liste trois types de traitements considérés comme nécessaires pour des motifs d'intérêt public important, tels les traitements effectués par les associations de défense des droits fondamentaux.

Pour le traitement des données génétiques, des données biométriques et des données concernant la santé, la loi-cadre requiert des mesures de protection plus strictes[128]. Il convient de désigner, dans une liste tenue la disposition de

125 Art. 9, § 2, a) à j), R.G.P.D. Les hypothèses b, g, h, i et j exigent l'adoption d'une norme apportant des garanties appropriées.

126 Pour un commentaire sur ces exceptions, voy. J.-M. Van Gyseghem, «Les catégories particulières de données», *in* C. de Terwangne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie, op. cit.*, p. 271. Voy. aussi Fr. Henry et I. Verhelst, «Protection des données à caractère personnel dans les relations individuelles et collectives de travail», dans le présent ouvrage.

127 Art. 9, § 2, g), R.G.P.D.

128 Art. 9 de la loi-cadre. Ces conditions sont reprises de l'ancien article 25 de l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992. B. Salovic, O. Guerguinov et Th. Léonard, «La Belgique transpose (enfin) le RGPD (GDPR)», 5 septembre 2018, www.droit-technologie.org/actualites/belgique-transpose-enfin-rgpd-gdpr/.

l'A.P.D., les catégories de personnes ayant accès aux données à caractère personnel, et de lier ces personnes par une obligation de confidentialité[129].

B. Les données relatives aux condamnations pénales et aux infractions

Une deuxième catégorie de données sensibles bénéficie d'un régime de protection particulièrement restrictif, même s'il est un peu plus ouvert que sous l'empire de la loi de 1992. Il s'agit des données à caractère personnel relatives aux condamnations pénales et aux infractions ou mesures de sûreté connexes[130].

L'article 10 du R.G.P.D. stipule que le traitement de ces données ne peut être effectué que sous le contrôle de l'autorité publique ou si le traitement est autorisé par le droit de l'Union ou par le droit d'un État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées.

L'article 10 de la loi-cadre prévoit en conséquence que le traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions pénales ou aux mesures de sûreté connexes peut être effectué :

1° par des personnes physiques ou morales pour autant que la gestion de leurs propres contentieux l'exige ;
2° par des avocats ou d'autres conseils juridiques, pour autant que la défense de leurs clients l'exige ;
3° par d'autres personnes[131] lorsque le traitement est nécessaire pour des motifs d'intérêt public important pour l'accomplissement de tâches d'intérêt général confiées par ou en vertu d'une loi, d'un décret, d'une ordonnance ou du droit de l'Union européenne. À titre d'exemple, on citera le projet de création d'une base de données centralisée pour la Région wallonne en matière de délinquance environnementale, reprenant tous les faits constitutifs d'infractions environnementales[132] ;
4° pour les nécessités de la recherche scientifique, historique ou statistique ou à des fins d'archives. Cette formulation soulève la perplexité. L'intention originale du législateur était de ne permettre l'utilisation de données pénales

129 Pour un cas d'application de cette exigence de garantie supplémentaire, voy. A.P.D., avis n° 86/2018 du 26 septembre 2018 relatif à une demande d'avis concernant un projet d'arrêté royal fixant les critères d'agrément des psychologues cliniciens, ainsi que des maîtres de stage et services de stage et un projet d'arrêté royal fixant les critères d'agrément des orthopédagogues cliniciens, ainsi que des maîtres de stage et services de stage.

130 Art. 10 R.G.P.D.

131 Cette expression «par d'autres personnes» n'est pas opportune car elle signifie littéralement que les traitements visés à la troisième hypothèse ne sont effectués ni par des personnes physiques ou morales (1re hypothèse), ni par des avocats ou autres conseils juridiques (2e hypothèse). Il ne reste dès lors plus beaucoup de possibilités… Cette expression est en fait une reprise de l'article 8, § 2, b, de la loi du 8 décembre 1992 où elle venait logiquement après la première hypothèse qui visait les traitements sous le contrôle d'une autorité publique ou d'un officier ministériel.

132 A.P.D., avis n° 87/2018 du 26 septembre 2018 concernant un avant-projet de décret wallon relatif à la délinquance environnementale.

qu'à des fins de recherche scientifique. C'était d'ailleurs la seule hypothèse admise dans la loi du 8 décembre 1992. La Commission vie privée a conseillé d'étendre l'accès aux données à la recherche historique et, pour soutenir ce type de recherche, aux traitements à des fins d'archivage dans l'intérêt public, en limitant l'accès des données aux seuls chercheurs[133]. Le Conseil d'État, lui aussi, a recommandé « dans un souci de proportionnalité, que le traitement de données archivées dans l'intérêt du public [soit] limité aux chercheurs »[134]. Toutefois, il a estimé qu'il fallait pouvoir justifier au regard du principe constitutionnel d'égalité la différence faite entre la finalité de recherche scientifique et les autres finalités (archivage et statistique). À défaut d'arriver à justifier cette différence, il a suggéré la formulation reprise finalement dans la loi. Il semble pourtant que l'on aurait pu justifier de restreindre l'accès des données particulièrement sensibles comme les données pénales aux seules fins de recherche scientifique (ça a été la règle pendant 27 ans…) ou d'archivage dans l'intérêt public, finalités liées à l'intérêt général, alors qu'on ne permettrait pas cet accès à des fins statistiques, qui ne sont pas nécessairement liées à l'intérêt général. Les utilisations de telles données dans le cadre du *big data*, par exemple, auquel il est fait intensément recours dans le secteur privé, s'apparentent à des traitements à des fins statistiques qui pourraient notamment déboucher sur des profilages discriminatoires non souhaitables s'ils intégraient les données pénales en question. La formule de « recherche statistique » n'est, en outre, pas claire et diffère des expressions utilisées par ailleurs. Enfin, les « fins d'archives » sont plus larges que les « fins archivistiques dans l'intérêt public ». Elles peuvent, comme les finalités statistiques, couvrir des situations qui n'ont plus de lien avec l'intérêt général ;

5° si la personne concernée a autorisé explicitement et par écrit le traitement de ces données à caractère personnel pour une finalité ou plusieurs finalités spécifiques et si leur traitement est limité à ces finalités ;

6° si le traitement porte sur des données à caractère personnel manifestement rendues publiques par la personne concernée, de sa propre initiative, pour une finalité ou plusieurs finalités spécifiques et si leur traitement est limité à ces finalités.

Les deux dernières hypothèses sont nouvelles dans le paysage belge de la protection des données.

L'exposé des motifs précise bien que cette liste n'est pas cumulative[135].

133 C.P.V.P., avis n° 33/2018 du 11 avril 2018 sur l'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, § 102.

134 S.L.C.E, avis n° 63.192/2 du 19 avril 2018 sur un 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. 450, p. 416. Mais cette limitation de l'accès aux données n'a pas été reprise par le législateur.

135 Exposé des motifs, préc., p. 22.

Le R.G.P.D. stipule encore que tout registre complet des condamnations pénales (le casier judiciaire) ne peut être tenu que sous le contrôle de l'autorité publique.

Pour toutes ces hypothèses dans lesquelles le traitement de données relatives aux condamnations pénales et aux infractions est autorisé, des mesures de sauvegarde supplémentaires sont requises, identiques à celles pour le traitement des données génétiques, biométriques ou de santé[136]. Le responsable du traitement et, le cas échéant, le sous-traitant sont ainsi tenus d'établir la liste des catégories de personnes ayant accès aux données en question, avec une description de leur fonction par rapport au traitement. Cette liste doit être tenue à la disposition de l'autorité de contrôle compétente. Les personnes désignées doivent être soumises à une obligation de confidentialité.

Enfin, les traitements de données effectués par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes, de poursuites et d'exécution de sanctions pénales sont désormais couverts par le titre 2 de la loi-cadre.

C. Les numéros d'identification uniques

Le R.G.P.D. s'en remet aux États membres pour décider d'autoriser l'utilisation d'un numéro d'identification unique ou de tout autre identifiant de portée générale[137]. Le texte impose toutefois, et c'est nouveau, aux États qui optent pour le recours à un tel identifiant de prévoir des garanties appropriées pour les droits et libertés de la personne concernée.

Section 5
Dispense d'identification des personnes concernées

Une disposition nouvelle particulièrement pertinente et bienvenue a été insérée dans le R.G.P.D. Il s'agit de l'article 11 selon lequel si les données traitées par un responsable du traitement ne permettent pas à celui-ci d'identifier une personne physique, il n'est pas obligé d'obtenir des informations supplémentaires pour identifier la personne en question à la seule fin de respecter le R.G.P.D. Cette disposition vise par exemple le cas où une caméra a été placée sur un immeuble filmant les allées et venues à l'entrée. Les images filmées sont des données à caractère personnel dès lors que les personnes sont identifiables, même si le propriétaire de l'immeuble ne procède pas lui-même à l'identification des personnes entrant et sortant. L'article 11 du R.G.P.D. dispense le responsable de ce traitement de chercher à obtenir l'identité des individus filmés

136 G. Rue, « La loi sur la protection des données est publiée », *B.J.S.*, 2018/615, p. 11.

137 Art. 87 R.G.P.D. Sur ce sujet, voy. la contribution d'É. Degrave dans le présent ouvrage.

juste pour être à même de leur répondre s'ils souhaitent exercer leurs droits d'accès, de rectification ou d'opposition. Dans le même sens, le chercheur qui travaille avec des données codées obtenues à diverses sources ne devra pas se fournir la clé des codes ni les informations de contact pour honorer son obligation d'information des personnes concernées.

L'idée est donc que les règles de protection des données n'aboutissent pas à la situation paradoxale où l'on doive en connaître davantage sur les personnes à propos de qui on traite des données pour garantir la protection de leurs données.

Section 6
Droits des personnes concernées

Toute personne concernée dispose désormais d'un véritable arsenal de droits dont l'exercice est renforcé[138].

A. Droit à l'information

1. Portée du droit

Tout responsable de traitement est tenu d'indiquer aux personnes concernées par les données qu'il traite son identité et ses coordonnées ainsi que celles de son représentant s'il en a un (dans le cas où il s'agit d'un responsable établi hors de l'Union européenne). Il doit également fournir les coordonnées de son délégué à la protection des données s'il en a un, ainsi que des informations sur les finalités du traitement, sur sa base de licéité (s'il s'agit de la balance d'intérêts – article 6, § 1er, f) – il doit en outre mentionner les intérêts légitimes liés à ce traitement), sur les catégories de destinataires des données et enfin, sur les intentions de transfert des données vers des pays tiers ou des organisations internationales, en indiquant s'il s'agit de destinations offrant une protection adéquate aux données transférées ou si les transferts sont encadrés par des garanties appropriées[139]. Ce devoir d'information s'impose, que la collecte des données s'effectue directement auprès de la personne concernée ou indirectement, auprès d'un tiers ou d'une autre source (auquel cas il faudra fournir aussi une information sur les catégories de données à caractère personnel traitées)[140].

138 Pour une présentation et analyse approfondie de l'ensemble des droits de la personne concernée, voy. Th. Tombal, «Les droits de la personne concernée dans le R.G.P.D.», *in* C. de Terwangne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, *op. cit.*, pp. 407 à 541.

139 Art. 13, § 1er, et 14, § 1er, R.G.P.D.

140 Art. 14, § 1er, d), R.G.P.D.

D'autres informations doivent ensuite être fournies lorsque cela est nécessaire pour garantir un traitement équitable et transparent : la durée de conservation des données ou à tout le moins les critères utilisés pour établir cette durée, l'existence d'un droit d'accès, de rectification et des autres droits, notamment le droit de retirer son consentement (si le traitement repose sur le consentement de la personne concernée), le caractère obligatoire ou non des réponses ainsi que les conséquences d'un défaut éventuel de réponse et, enfin, l'existence d'une décision automatisée ou d'un profilage, accompagnée d'informations concernant la logique sous-jacente et les conséquences découlant de cette décision automatisée ou de ce profilage pour la personne concernée[141].

L'article 14, § 4, du R.G.P.D. ajoute encore un nouvel élément au cas où le responsable du traitement aurait l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été obtenues[142]. Dans ce cas, ce responsable doit fournir, au préalable, des informations au sujet de cette autre finalité à la personne concernée. En particulier, il doit indiquer en quoi le traitement ultérieur est à ses yeux compatible avec la finalité du traitement originaire[143].

Pour que ce droit à être informé ne soit pas un leurre, le R.G.P.D. exige que les informations à fournir le soient de façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant[144]. La forme que doit prendre la démarche d'information est libre et peut donc être adaptée aux circonstances.

Cette formalité d'information doit être accomplie soit au moment de l'obtention des données (en cas de collecte directe auprès de la personne concernée), soit au plus tard au moment de la première communication des données, si les données ont été obtenues de manière indirecte.

141 Art. 13, § 2, et 14, § 2, R.G.P.D.

142 Voy. *supra*, les développements sur le principe de finalité.

143 Groupe 29, «Guidelines on transparency under Regulation 2016/679», 12 décembre 2017, WP 260, p. 20 ; Th. Tombal, «Les droits de la personne concernée dans le R.G.P.D.», *in* C. de Terwangne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, *op. cit.*, p. 423.

144 Art. 12, § 1er, R.G.P.D. Également Groupe de l'article 29, «Lignes directrices sur la transparence au sens du règlement (UE) nº 2016/679», 12 décembre 2017, révisée le 11 avril 2018, WP 260 rev. 01, disponible sur https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227. Voy. les développements sur les exigences de forme de la communication des données (qualité et moyens de cette communication) dans Th. Tombal, «Les droits de la personne concernée dans le R.G.P.D.», *op. cit.*, pp. 411 et s.

2. Exceptions

Le droit à l'information n'est bien sûr pas absolu et une série d'exceptions peuvent intervenir. Certaines exceptions figurent dans le R.G.P.D. tandis que d'autres ont été introduites par la loi-cadre. Là où c'est approprié, le responsable du traitement peut compenser l'absence d'information personnalisée en rendant les informations normalement requises publiquement disponibles[145].

Il ne faut pas communiquer l'ensemble des informations mentionnées ci-dessus si la personne concernée dispose déjà de ces informations[146]. Dans les seuls cas où les données ont été obtenues de source indirecte, les responsables des traitements de données sont en outre dispensés de fournir les informations requises dans l'hypothèse où l'information des personnes concernées se révèle impossible ou implique des efforts disproportionnés[147], ou si cette information est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement[148] ou encore lorsque l'obtention ou la communication des données à caractère personnel sont expressément prévues par le droit de l'Union ou le droit belge.

Lorsqu'une obligation légale de secret professionnel intervient, les données à caractère personnel peuvent être traitées sans que le traitement fasse l'objet de mesures d'information à l'égard des personnes concernées[149]. C'est le cas d'un avocat à qui le client confie un nombre d'informations sur des tiers (p. ex., sur la conjointe dont le client veut divorcer ou sur l'employeur avec qui le client est en litige). Il est clair que l'avocat ne peut prévenir ces tiers du traitement de leurs données, sous peine de violation de son secret professionnel.

En sus des exceptions contenues dans le R.G.P.D., la loi-cadre prévoit à ses articles 11 à 17 ainsi qu'aux titres 2 et 3 des dérogations aux droits des personnes concernées, en cas d'enquête pénale ou des services de sécurité.

B. Droit d'accès

Le droit d'accès offre à la personne concernée une autre voie pour obtenir des informations sur les traitements effectués sur ses données, voie qui exige une démarche de sa part. Sous l'appellation « droit d'accès » c'est un ensemble de prérogatives qui sont garanties à la personne concernée : droit à la curiosité, droit d'obtenir gratuitement une copie des données traitées[150], droit d'accès aux

145 Art. 14, § 5, b), R.G.P.D.
146 Art. 13, § 4, R.G.P.D.
147 Art. 14, § 5, b), R.G.P.D.
148 Art. 14, § 5, b), R.G.P.D.
149 Art. 14, § 5, d), R.G.P.D.
150 La chambre contentieuse de l'A.P.D. a été saisie de la plainte d'une patiente ayant demandé en vain l'accès à et la suppression de ses données utilisées à des fins de campagne électorale par l'administratrice de l'A.S.B.L. assurant les soins infirmiers. La chambre contentieuse a estimé que la nature du traitement (réutilisation de données médicales hors du contexte de soins) implique que le manquement aux articles 12, 3., et 15 du R.G.P.D. est grave. En conséquence elle a fixé l'amende administrative à 2.000 euros (A.P.D., ch. contentieuse, décision 13/2019 du 17 décembre 2019, § 26).

informations sur l'origine des données, sur leurs destinataires et sur la logique ou le raisonnement qui sous-tend le traitement automatisé des données[151]. À l'heure où il est de plus en plus recouru à des algorithmes, ce dernier « exercice de vulgarisation de la logique qui sous-tend le processus de traitement peut se révéler particulièrement complexe »[152]. On ajoutera encore que toutes les données ou informations sollicitées doivent être transmises dans le mois.

Le droit d'obtenir une copie des données ne doit pas porter atteinte aux droits et libertés d'autrui. Le considérant 63 du R.G.P.D. précise que les « droits et libertés d'autrui » comprennent le secret des affaires et la propriété intellectuelle, notamment le droit d'auteur protégeant le logiciel. Ce considérant ajoute toutefois une précision cruciale pour garder au droit d'accès toute sa portée : « Cependant, ces considérations ne devraient pas aboutir à refuser toute communication d'informations à la personne concernée ». Ainsi, plutôt que donner une copie du document original contenant les données à caractère personnel, dans le cas où cela porterait atteinte au secret d'affaires ou au droit d'auteur du document original, il convient de fournir une copie des données extraites du document[153].

En revanche, il est des cas où il ne sera pas possible de donner accès aux données. Il s'agit des situations dans lesquelles la protection des droits et libertés d'autrui l'emporte sur toute communication des données. Ainsi, dans le cas où des données relatives à une personne figurent dans un échange de mails entre deux collègues, il n'est en principe pas question de laisser la personne mentionnée dans le message accéder à ce qui se dit sur elle. Le secret des communications, protégé notamment par l'article 8 de la C.E.D.H. et par l'article 7 de la Charte des droits fondamentaux de l'Union européenne, s'oppose à une telle ingérence.

En outre, des limitations au droit d'accès sont prévues dans la loi-cadre pour les traitements liés aux enquêtes et poursuites pénales ou aux missions des services de sécurité et autres autorités visées par les articles 11 à 17 ainsi que par les titres 2 et 3 de la loi-cadre, pour les traitements poursuivant une finalité journalistique, universitaire, artistique ou littéraire et enfin pour les traitements à des fins statistiques, historiques ou de recherche scientifique.

151 Art. 15 R.G.P.D. Pour de plus amples développements sur ce droit, voy. C. DE TERWANGNE, « Le droit d'accès : un accès "riche" », *in* C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique – Manuel de base*, *op. cit.*, pp. 67 et s.
152 C. PONSART et R. ROBERT, « Le règlement européen de protection des données personnelles », *op. cit.*, p. 427.
153 Voy. Th. TOMBAL, « Les droits de la personne concernée dans le RGPD », *op. cit.*, p. 440.

C. Droit de rectification

L'individu concerné par les données se voit reconnaître un droit de rectification des données inexactes[154]. S'y ajoute le droit pour la personne concernée d'obtenir que les données à caractère personnel incomplètes compte tenu des finalités du traitement soient complétées, y compris en fournissant une déclaration complémentaire[155].

À l'instar de tous les autres droits, ce droit s'exerce gratuitement.

Aux termes de l'article 19 du R.G.P.D., le responsable du traitement est tenu de notifier à chaque destinataire auquel les données à caractère personnel ont été communiquées toute rectification ou toute limitation du traitement effectuée. Cette obligation de faire suivre les corrections est précieuse car elle permet de stopper la divulgation d'informations fausses ou incomplètes. Le responsable du traitement est toutefois dispensé de cette notification si celle-ci se révèle impossible ou exige des efforts disproportionnés. Le responsable doit fournir à la personne concernée des informations sur ces destinataires si celle-ci en fait la demande.

Comme pour les autres droits, des limitations au droit de rectification sont prévues dans la loi-cadre[156].

D. Droit à l'effacement ou droit à l'oubli

L'article 17 du R.G.P.D. reconnaît aux personnes concernées le droit à l'effacement, assimilé au « droit à l'oubli », notion qui a fait couler beaucoup d'encre et suscité de nombreux débats[157].

Toute personne concernée peut, sans frais, faire effacer dans les meilleurs délais les données à caractère personnel qui se rapportent à elle « lorsque la conservation de ces données constitue une violation du présent règlement »[158]. Ce droit à l'effacement est en particulier valable lorsqu'une personne retire son consentement donné antérieurement. Ce droit de changer d'avis et de revenir

154 Art. 16 R.G.P.D.

155 *Ibid.*

156 *Cf. supra*, pt B.

157 Voy. E. Cruysmans, « La réputation en ligne : droit de réponse, droit de rectification et droit à l'oubli », *in* Q. Van Enis et C. de Terwangne (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, *op. cit.*, p. 413 ; E. Cruysmans et A. Strowel, « Un droit à l'oubli face aux moteurs de recherche : droit applicable et responsabilité pour le référencement de données "inadéquates, non pertinentes ou excessives" », *J.T.*, 2014, p. 451 ; E. Defreyne et R. Robert, « L'arrêt "Google Spain" : une clarification de la responsabilité des moteurs de recherche … aux conséquences encore floues », *R.D.T.I.*, 2014/3, pp. 73 à 114 ; C. de Terwangne, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique », *in* A. Grosjean, *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, pp. 237 à 268 ; A. Cassart et J.-Fr. Henrotte, « Arrêt *Google Spain* : la révélation d'un droit à l'effacement plutôt que la création d'un droit à l'oubli », *J.L.M.B.*, 2014, pp. 1168 et s.

158 Cons. 65 R.G.P.D.

sur ce qu'on avait accepté sans peut-être envisager toutes les conséquences est particulièrement important dans le contexte d'aujourd'hui. Il est aussi précieux lorsqu'on en vient à regretter ce qu'on a exprimé ou diffusé grâce à l'interactivité du web. De telles situations sont malheureusement fréquentes quand l'expression est spontanée et impulsive, comme c'est souvent le cas sur les sites de réseaux sociaux, et spécialement quand celui qui s'exprime est jeune.

L'article 17 énonce d'autres hypothèses dans lesquelles s'applique le droit à l'oubli et à l'effacement : celle où il revient au responsable d'effacer les données qui ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées, celle où la personne concernée s'oppose au traitement de ses données, celle qui se présente en cas de traitement illicite des données, traitement qui ne respecte donc pas les exigences du R.G.P.D. (les données sont par exemple incomplètes, non pertinentes ou excessives au regard de la finalité du traitement), celle où la loi impose l'effacement des données, et enfin celle où les données ont été collectées quand la personne était un enfant.

L'article 17, § 2, a étendu le droit à l'effacement « de façon à ce que le responsable du traitement qui a rendu les données à caractère personnel publiques soit tenu d'informer les responsables du traitement qui traitent ces données à caractère personnel qu'il convient d'effacer tout lien vers ces données, ou toute copie ou reproduction de celles-ci. Ce faisant, ce responsable du traitement devrait prendre des mesures raisonnables, compte tenu des technologies disponibles et des moyens dont il dispose, y compris des mesures techniques afin d'informer les responsables du traitement qui traitent les données à caractère personnel de la demande formulée par la personne concernée »[159].

Le droit à l'effacement et à l'oubli n'est bien sûr pas absolu et, dans une série de cas, notamment lorsque ce droit se heurte à l'exercice de la liberté d'expression ou à l'exécution d'une mission d'intérêt public, le traitement des données pourra se poursuivre. Pour faciliter la tâche du responsable du traitement, en première ligne pour réaliser la pondération des intérêts, mais aussi pour éclairer les autorités appelées éventuellement à (in)valider cette mise en balance, le Groupe de l'article 29 a publié des lignes directrices proposant des critères uniformes[160].

Outre ces exceptions, les limitations prévues par la loi-cadre pour les traitements en matière de police-justice, sécurité publique et pour des finalités journalistique, universitaire, artistique ou littéraire sont aussi d'application.

159 *Ibid.*

160 Groupe de l'article 29, « Guidelines on the implementation of the Court of Justice of the European Union judgment on *"Google Spain and inc. v. Agencia Española de Protección de Datos (A.E.P.D.) and Mario Costeja González"* C-131/121 », 26 novembre 2014, WP 225.

E. Droit d'opposition

Lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, ou en raison des intérêts légitimes du responsable du traitement ou d'un tiers, la personne dont les données sont traitées peut s'opposer au traitement[161]. Elle devra uniquement démontrer qu'elle a « des raisons tenant à sa situation particulière » pour obtenir la cessation du traitement de ses données. C'est au responsable du traitement qu'il incombera de prouver que ses intérêts légitimes et impérieux prévalent sur les intérêts de la personne concernée s'il veut poursuivre le traitement[162].

Si le traitement est réalisé à des fins de prospection (marketing direct p. ex.), la personne concernée pourra s'y opposer sans justification aucune et aucune réplique n'est permise pour le responsable du traitement[163].

F. Droit à la limitation du traitement

Au sens du R.G.P.D., la limitation du traitement est « le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur »[164]. La limitation du traitement engendre une interdiction de traiter les données (à moins d'avoir obtenu le consentement de la personne concernée), à l'exception de la conservation de celles-ci ou pour la constatation, l'exercice ou la défense de droits en justice entre autres[165]. C'est principalement en cas d'activation du droit de rectification des données (pendant la durée de contestation de l'exactitude des données) ou du droit d'opposition au traitement (pendant le temps nécessaire à la vérification de ce que les motifs légitimes poursuivis par le responsable du traitement prévalent ou non sur ceux de la personne concernée)[166] que le traitement des données en cause sera limité. Le droit à la limitation du traitement est un droit essentiellement temporaire et circonstanciel[167].

161 Art. 21 R.G.P.D.
162 Cons. 69 R.G.P.D.
163 Art. 21, § 2, R.G.P.D.
164 Art. 4, 3, R.G.P.D.
165 Art. 18, § 1er, R.G.P.D. et cons. 67 R.G.P.D.
166 Art. 16, § 1er, a) et d), R.G.P.D.
167 Th. Léonard et D. Chaumont, GDPR.expert, « Article 18. Droit à la limitation du traitement », www.gdpr-expert.eu/article.html?id=18#eu-regulation ; E. Cruysmans, « La réputation en ligne : droit de réponse, droit de rectification et droit à l'oubli », *in* Q. Van Enis et C. de Terwangne (dir.), *L'Europe des droits de l'homme à l'heure d'Internet*, *op. cit.*, p. 416.

G. Droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage

L'homme ne doit pas être soumis à la machine. Au nom de la dignité humaine, il est inadmissible qu'une décision qui s'impose à un individu dépende des seules conclusions d'une machine. L'article 22 du R.G.P.D. reconnaît à la personne concernée « le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage[168], produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire ». Le responsable du traitement ne peut pas prendre de décision fondée uniquement sur un traitement automatisé ou du profilage et qui affecte la personne de manière significative ou qui produit des effets juridiques à l'encontre de celle-ci. Sont à titre d'exemple considérés comme tels, le rejet automatique d'une demande de crédit en ligne ou des pratiques de recrutement en ligne ne nécessitant aucune intervention humaine[169].

Des exceptions à l'interdiction sont prévues lorsque la décision automatisée est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne et le responsable du traitement ; lorsqu'elle est autorisée par une disposition légale prévoyant des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ; lorsque la personne concernée a consenti explicitement à ce qu'une décision de ce type soit prise à son égard[170]. Dans la première et la dernière hypothèse, le responsable du traitement devra au minimum permettre à la personne concernée d'obtenir l'intervention d'une personne, d'exprimer son point de vue ainsi que de contester la décision automatisée[171].

Les décisions individuelles automatisées admises ne peuvent toutefois pas être fondées sur des données sensibles, à moins que la personne ait donné son consentement explicite ou que ce soit nécessaire pour des motifs d'intérêt public important et que des mesures appropriées de sauvegarde soient prises[172].

Comme pour les autres droits, les exceptions prévues dans la loi-cadre peuvent également trouver à s'appliquer.

168 L'article 4, 4, du R.G.P.D. définit le profilage comme « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».
169 Cons. 71 R.G.P.D. ; voy. également A. Grosjean, « Le profilage : un défi pour la protection des données à caractère personnel », *in Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, p. 302.
170 Art. 22, § 2, R.G.P.D.
171 Art. 22, § 3, R.G.P.D.
172 Art. 22, § 4, R.G.P.D.

H. Droit à la portabilité des données

Enfin, le R.G.P.D. garantit aux personnes concernées un nouveau droit : le droit à la portabilité des données[173]. Aux termes de l'article 20, en cas de traitement automatisé de données fondé sur un contrat ou sur le consentement de la personne concernée, cette dernière a le droit de recevoir du responsable du traitement les données à caractère personnel qu'elle a fournies[174], « dans un format structuré, couramment utilisé et lisible par machine », afin de transmettre ces données à un autre responsable du traitement. Lorsque cela est techniquement possible, le responsable du traitement devra transmettre lui-même, à la demande de la personne concernée, les données directement à un autre responsable du traitement[175].

Néanmoins, l'étendue du droit à la portabilité des données sera inévitablement limitée lorsque plusieurs personnes sont concernées par un ensemble de données à caractère personnel. En effet, le quatrième paragraphe de l'article 20 stipule que « le droit [à la portabilité des données] ne porte pas atteinte aux droits et libertés des tiers ».

La création de ce nouveau droit à la portabilité est liée à l'apparition des réseaux sociaux[176]. Elle témoigne « de la volonté claire d'éviter que les personnes concernées ne soient "coincées"[177] par les géants actuels tels que Facebook ou Google, en permettant à ces personnes de "porter" les données à caractère personnel qu'elles avaient fournies à ces géants vers un nouveau service alternatif en ligne. De fait, en l'absence d'un tel droit, l'on pourrait tout à fait imaginer que la personne concernée s'abstienne de faire usage d'un tel service alternatif, se résignant, par exemple, à rester "fidèle" à Facebook, au vu de l'investissement temporel substantiel que représenterait, pour cette personne concernée, le fait d'ajouter elle-même, sur ce nouveau service, l'ensemble des données à caractère personnel qu'elle aurait déjà "uploadé" sur Facebook (informations personnelles, photos, etc.) »[178].

173 Voy. Groupe de l'article 29, « Guidelines on the right to data portability », 13 avril 2017, WP 242 rev.01 ; Th. Tombal, « Les droits de la personne concernée dans le R.G.P.D. », *op. cit.*, pp. 482 et s. ; I. Graef, M. Husovec, N. Purtova, « Data portability and data control: Lessons for an emerging concept in EU law », *German Law Journal*, 2018, *19*(6), pp. 1359 à 1398 ; J.-N. Colin et M. Knockaert, « Le droit à la portabilité des données à caractère personnel : coup d'œil juridique et technique », *DPO News*, 2019/1, pp. 3 à 5.

174 Sur la notion de « données fournies », voy. P. Valcke et J. Verschakelen, « Dataportabiliteit en digitale (mensen-)handel », *N.J.W.*, 9 avril 2014, pp. 298 à 300 ; C. de Terwangne, K. Rosier et B. Losdyck, « Lignes de force du nouveau règlement relatif à la protection des données à caractère personnel », *R.D.T.I.*, 2016/62, p. 48, § 90.

175 Art. 20, § 2, R.G.P.D.

176 D. de Bot, « De uitvoering van de algemene verordening gegevensbescherming – Enkele bemerkingen bij de Belgische context », *T.V.W.*, 2016/3, p. 221.

177 « *Lock-in* ».

178 Th. Tombal, « Les droits de la personne concernée dans le R.G.P.D. », *op. cit.*, p. 484.

Comme pour les autres droits, les exceptions prévues dans la loi-cadre peuvent également trouver à s'appliquer.

Section 7

Obligations des acteurs

Les principaux acteurs, c'est-à-dire le responsable du traitement – voire les coresponsables – et son éventuel sous-traitant, voient peser sur eux des obligations nouvelles ou alourdies. Par l'application du principe d'*accountability* (*cf. supra*), ils doivent être en mesure de démontrer à tout instant leur conformité avec ces obligations.

A. Obligation de protection dès la conception et par défaut

Si la protection des individus à l'égard du traitement de leurs données est inscrite dans des règles juridiques, elle se réalise en s'appuyant aussi sur des dispositifs techniques. Le R.G.P.D. exige[179] que les équipements et applications qui traitent les données soient à l'origine conçus et paramétrés pour tenir compte des enjeux en matière de protection des données.

Le principe de la protection des données dès la conception impose au responsable du traitement de tenir compte des règles de protection des données dans le processus même de développement du traitement. Le responsable du traitement doit concevoir celui-ci de manière à assurer la mise en œuvre des règles de protection des données. Il doit mettre en œuvre, « tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du [R.G.P.D.] et de protéger les droits de la personne concernée »[180]. « Ainsi, il faut prévoir, dès le début, dans le cahier des charges, que le logiciel utilisé pour ces traitements doit être capable d'effacer certaines données (droit à l'effacement…) ou d'exporter ces données (droit à la portabilité), qu'il doit être sécurisé, qu'il ne nécessite pas le traitement de données à caractère personnel inutilement[181]… »[182].

L'obligation de protection par défaut « est une forme particulière du principe de *privacy by design* »[183]. Le responsable du traitement doit adopter des

179 Art. 25 R.G.P.D.

180 Art. 25, § 1er, R.G.P.D.

181 Voy. cons. 78 R.G.P.D.

182 A. Delforge, « Les obligations du responsable de traitement et du sous-traitant », *in* C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique – Manuel de base*, *op. cit.*, pp. 82 et s.

183 *Ibid.*, p. 83.

mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Le R.G.P.D. ajoute que « cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité »[184]. Au niveau de l'accessibilité particulièrement, il faut veiller à ce que les mesures prises garantissent, par défaut, que les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes sans que la personne concernée ne soit invitée à intervenir en ce sens.

B. La tenue d'un registre des activités de traitement

Une obligation documentaire a remplacé l'obligation de déclaration préalable qui était contenue dans la directive 95/46 et la loi de 1992 (et qui alimentait un registre public des déclarations, disponible sur le site web de la Commission vie privée). Aux termes de l'article 30 du R.G.P.D., le responsable du traitement doit tenir un registre des activités de traitement effectuées sous sa responsabilité. Il s'agit d'identifier dans un document écrit les caractéristiques des traitements énoncées dans le R.G.P.D. (finalités, catégories de données traitées, catégories de personnes concernées…) et de tenir ce document à disposition de l'autorité de contrôle[185]. Les sous-traitants doivent, quant à eux, tenir un registre des catégories d'activités de traitement.

Sont exemptées de cette obligation les organisations ou entreprises qui comptent moins de 250 employés. Cette exemption tombe toutefois si le traitement est susceptible de comporter un risque pour les droits et libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les données sensibles.

C. L'analyse d'impact

Avant de se mettre à traiter des données à caractère personnel, le responsable du traitement a l'obligation, dans certains cas, de procéder à une analyse des risques que présente le traitement envisagé sur les droits et libertés fondamentales d'autrui[186]. Cette analyse appelée « analyse d'impact relative à la protection des données » (A.I.P.D. – ou « *privacy impact assessment* », PIA) vise à déterminer les mesures à prendre pour prévenir le ou les risques identifiés.

184 Art. 25, § 2, R.G.P.D.

185 C.P.V.P., Recommandation n° 06/2017 relative au Registre des activités de traitements, 14 juin 2017. Pour un modèle de registre, voy. celui élaboré par l'A.P.D. et reprenant une liste préétablie d'éléments fréquemment utilisés, www.autoriteprotectiondonnees.be/node/20442 ou le modèle de la CNIL française, www.cnil.fr/fr/rgpd-le-registre-des-activites-de-traitement.

186 Art. 35 R.G.P.D. Voy. A. Delforge, « Les obligations du responsable de traitement et du sous-traitant », *in* C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique – Manuel de base*, *op. cit.*, pp. 99 et s.

Aux termes de l'article 35, § 1er, du R.G.P.D., l'analyse d'impact s'impose lorsque « un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques ».

Le R.G.P.D. ne définit pas la notion de « risque élevé » mais identifie trois hypothèses dans lesquelles l'analyse est d'office requise : (i) la surveillance systématique à grande échelle d'une zone accessible au public, (ii) le traitement à grande échelle de données sensibles ainsi que (iii) en cas d'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire. Ce dernier cas de figure vise par exemple le traitement de *big data*. Au-delà de ces trois cas, l'A.P.D. a établi une liste de huit cas dans lesquels la réalisation d'une A.I.P.D. est obligatoire[187].

L'analyse de risques doit être documentée et conduire à la réalisation d'un document écrit dont le contenu minimum est arrêté à l'article 35, § 7, du R.G.P.D.

L'A.P.D. doit être consultée si l'A.I.P.D. indique que le risque résiduel du traitement envisagé reste élevé[188].

D. L'obligation de sécurité

1. Mesures de sécurité appropriées

Il est impératif de protéger les données à caractère personnel contre une curiosité malsaine venant de l'intérieur ou de l'extérieur ou contre des manipulations non autorisées ou illicites, qu'elles soient de nature accidentelle ou qu'elles soient malintentionnées. Un devoir d'adopter des mesures de sécurité existait déjà dans la directive 95/46. Il a été repris à l'article 32 du R.G.P.D. avec, au passage, une clarification de la responsabilité de la sécurité : elle revient au responsable du traitement ainsi qu'à son sous-traitant dans les cas où il est recouru aux services d'un sous-traitant.

187 A.P.D., décision 1/2019 du 16 janvier 2019, Adoption de la liste des catégories de traitement devant faire l'objet d'une analyse d'impact relative à la protection des données conformément à l'article 35.4 du Règlement général sur la protection des données. Voy. également les neuf critères proposés par le Groupe de l'article 29 pour évaluer le caractère « élevé » du risque (Groupe de l'article 29, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (A.I.P.D.) et la manière de déterminer si le traitement est "susceptible d'engendrer un risque élevé" aux fins du règlement (UE) n° 2016/679 », 4 avril 2017, modif. le 4 octobre 2017, WP 248 rév. 01).

188 Art. 36 R.G.P.D. Voy. C.P.V.P., recommandation d'initiative 01/2018 du 28 février 2018 concernant l'analyse d'impact relative à la protection des données et la consultation préalable.

Ces acteurs doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, « compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques »[189]. L'exigence de sécurité est donc modalisable en fonction des risques que le traitement fait courir aux personnes concernées. Ainsi, plus les données en cause sont sensibles et les risques pour la personne concernée grands, plus importantes seront les précautions à prendre. Par exemple, des données relatives à la santé d'une personne, utilisées en dehors d'un contexte médical (p. ex., par une compagnie d'assurances pour octroyer une assurance-vie ou par un avocat pour la défense d'un client), devront être encadrées de mesures de sécurité sévères.

Les mesures de sécurité à prendre sont de deux ordres : des mesures organisationnelles (limiter le nombre de personnes ayant accès aux données, utiliser des mots de passe renouvelés régulièrement, fermer les locaux où sont localisés les ordinateurs ou les fichiers, etc.) et des mesures techniques (programme antivirus fréquemment mis à jour, *firewalls*, *back-up* de sécurité, *login*…).

2. Notification des violations de données à caractère personnel

Malgré la mise en place de mesures de sécurité, aucun responsable de traitement n'est à l'abri d'une perte de données (surtout sur des supports mobiles ou portables) ou d'une faille de sécurité, les *hackers* faisant sans cesse preuve d'inventivité pour pénétrer les systèmes informatiques. De telles failles de sécurité peuvent entraîner la perte, l'altération ou la divulgation de données personnelles et être préjudiciables tant pour l'individu que pour le responsable du traitement.

Aux termes des articles 33 et 34 du R.G.P.D., les responsables de traitement ont l'obligation de notifier les violations de données à caractère personnel dont ils sont victimes. C'est une des grandes nouveautés apportées par le R.G.P.D. Ces violations s'entendent de toute « violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données »[190].

Le responsable du traitement doit notifier la violation de données à l'A.P.D., « dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible

189 Art. 32, § 1er, R.G.P.D.
190 Art. 4, 12°, R.G.P.D.

d'engendrer un risque pour les droits et libertés des personnes physiques »[191]. Seules les violations susceptibles de porter atteinte aux droits et libertés des personnes concernées doivent donc être notifiées par le responsable du traitement à l'autorité[192]. Il devra néanmoins répertorier et documenter toutes les violations dans un registre, de façon à ce que les autorités de contrôle puissent évaluer le respect de l'article 33 relatif aux violations de données[193]. Le R.G.P.D. fait donc reposer sur le responsable du traitement la délicate question de savoir si une violation de données est susceptible de porter atteinte aux droits et libertés des individus[194], évaluation qui pourra *a posteriori* faire l'objet d'un contrôle de la part de l'A.P.D.[195].

De plus, la violation de données devra également être communiquée dans les meilleurs délais aux individus concernés si elle engendre un risque élevé pour leurs droits et libertés, à moins que le responsable du traitement ait appliqué aux données affectées des mesures de protection appropriées, en particulier des mesures qui rendent les données à caractère personnel incompréhensibles (p. ex., grâce à la cryptographie), ou que le risque élevé ait été maitrisé par le responsable du traitement[196]. Toutefois, si une telle communication devait demander des efforts disproportionnés, le responsable du traitement pourrait procéder à une communication publique ou recourir à tout autre moyen permettant d'informer les personnes concernées[197].

Par ailleurs, si le sous-traitant n'a pas l'obligation de notifier une violation de données à l'autorité de contrôle contrairement au responsable du traitement, il doit néanmoins notifier les violations de données dont il est victime au responsable du traitement dans les meilleurs délais[198]. Le responsable du traitement doit donc veiller à ce que ses sous-traitants lui transmettent les documents détaillant les violations de données qu'ils ont subies. En effet, une obligation de documentation de chaque violation de données pèse sur le responsable du traitement.

191 Art. 33, § 1er, R.G.P.D.
192 Voy. les exemples mentionnés dans Groupe de l'article 29, « Guidelines on Personal data breach notification under Regulation 2016/679 », 3 octobre 2017, rév. le 6 février 2018, WP 250 rev.01.
193 Art. 33, § 5, R.G.P.D.
194 Sur la manière d'évaluer le risque engendré par une violation, voy. F. Dumortier, « La sécurité des traitements de données, les analyses d'impact et les violations de données », *op. cit.*, pp. 243 et s.
195 C. de Terwangne, K. Rosier et B. Losdyck, « Lignes de force du nouveau règlement relatif à la protection des données à caractère personnel », *R.D.T.I.*, 2016/62, p. 35, n° 57.
196 Art. 34, § 1er, R.G.P.D.
197 Art. 34, § 3, c), R.G.P.D.
198 Art. 33, § 2, R.G.P.D.

E. La nomination d'un délégué à la protection des données

Un nouvel acteur est apparu depuis l'avènement du R.G.P.D., recruté par milliers à travers l'Europe et le monde : le délégué à la protection des données (*data protection officer*)[199].

Sa désignation par le responsable du traitement ou par le sous-traitant est obligatoire ou optionnelle selon le cas. Le R.G.P.D. impose une telle désignation en présence de traitements effectués par une autorité publique[200] ou un organisme public, exception faite toutefois des juridictions agissant dans l'exercice de leur fonction juridictionnelle[201]. Dans le secteur privé, la désignation d'un délégué à la protection des données est requise lorsque les activités de base du responsable du traitement ou du sous-traitant (et donc pas lorsque les traitements ne sont effectués qu'en tant qu'activité auxiliaire) consistent (i) 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 ou encore (ii) en un traitement à grande échelle de données sensibles ou judiciaires[202]. Le R.G.P.D. a laissé la possibilité aux États membres ou au droit de l'Union d'imposer la désignation d'un délégué dans d'autres hypothèses[203]. Le législateur belge a saisi l'occasion et impose pareille désignation à « l'organisme privé qui 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 [...] lorsque le traitement de ces données peut engendrer un risque élevé tel que visé à l'article 35 du règlement »[204].

En dehors de ces cas de nomination obligatoire, tout responsable de traitement ou sous-traitant peut s'adjoindre les services d'un délégué à la protection des données. En ce cas, les règles du R.G.P.D. concernant le D.P.O. s'appliquent au délégué en question, notamment en ce qui concerne la protection contre un licenciement ou une rupture de contrat[205].

Le D.P.O. doit informer et conseiller le responsable du traitement ou le sous-traitant qui l'a désigné et servir de point de contact avec l'autorité de

199 Art. 37 R.G.P.D. La notion n'est toutefois pas tout à fait neuve. Elle était déjà mentionnée au chapitre 8 du règlement n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données. Sur la notion et le rôle du D.P.O., voy. K. Rosier, « Délégué à la protection des données : une fonction multifacette », *in* C. de Terwangne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, *op. cit.*, pp. 559 et s.

200 Voy. art. 5 de la loi-cadre.

201 Art. 37, § 1er, a). Voy. Groupe de l'article 29, « Lignes directrices concernant les délégués à la protection des données (D.P.D.) », 13 décembre 2016, rév. le 5 avril 2017, WP 243 rev.01, p. 8.

202 Art. 37, § 1er, a) et b), et cons. 97 R.G.P.D.

203 Art. 37, § 4, R.G.P.D.

204 Art. 21 de la loi-cadre.

205 Art. 37, §§ 1er et 4, R.G.P.D.

contrôle ou des personnes concernées[206]. Il peut être un membre du personnel ou un tiers prestant dans le cadre d'un contrat de services[207]. Le R.G.P.D. impose des garanties pour que le délégué puisse avoir une connaissance effective des activités de traitement et travailler de manière indépendante et sans crainte de se voir sanctionner pour les avis ou conseils qu'il donne[208]. Le délégué ne peut notamment être pénalisé ou relevé de ses fonctions pour l'exercice de ses fonctions.

F. Les contrats entre le responsable du traitement et ses partenaires – Les protocoles avec les acteurs publics

Dans de nombreux cas, le responsable du traitement ne se retrouve pas seul en jeu. Soit il a partagé avec d'autres les décisions quant aux finalités et aux moyens du traitement et on est en présence de plusieurs responsables du traitement conjoints. Soit il a externalisé certaines tâches ou certains aspects du traitement en faisant appel à un sous-traitant.

Le R.G.P.D. impose la rédaction de contrats entre ces différents acteurs liés. Si l'on est en présence de responsables conjoints, ces derniers doivent obligatoirement rédiger un contrat dans lequel sont précisés le rôle et les devoirs de chacun[209].

Dans les hypothèses de sous-traitance, le responsable du traitement doit conclure un contrat avec son sous-traitant, en veillant à inclure dans ce contrat tous les éléments listés à l'article 28, § 3, du R.G.P.D. Parmi ces éléments figurent l'obligation pour le sous-traitant de ne traiter les données à caractère personnel que sur instruction documentée du responsable de traitement (ce qui n'empêche pas qu'il doit informer immédiatement le responsable du traitement s'il estime qu'une instruction qui lui est donnée constitue une violation du R.G.P.D.[210]), l'obligation d'aider le responsable du traitement dans la suite à donner à l'exercice des droits des personnes concernées, l'obligation d'assistance dans l'analyse d'impact, et l'obligation de supprimer ou de restituer les données traitées à la fin de la mission de sous-traitance[211]. Cette liste reflète l'extension des obligations mises à charge du sous-traitant par le R.G.P.D.

206 Art. 37, § 5, R.G.P.D. Pour les fonctions du délégué, voy. art. 39, § 1er, R.G.P.D.

207 Art. 37, § 6, R.G.P.D.

208 Art. 38, §§ 2 et 3, R.G.P.D. Pour une présentation détaillée, voy. A. Delforge, « Les obligations du responsable de traitement et du sous-traitant », *op. cit.*, pp. 90 et s.

209 Art. 26, § 1er, R.G.P.D.

210 Art. 28, § 3, h), al. 2, R.G.P.D.

211 Pour de plus amples développements, voy. A. Delforge, « Les obligations du responsable de traitement et du sous-traitant », *op. cit.*, pp. 85 et s.; A. Delforge, « Les obligations générales du responsable de traitement et la place du sous-traitant », *in* C. de Terwangne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, *op. cit.*, pp. 371 et s.; A. Cruquenaire et J.-Fr. Henrotte, « Le devoir de conseil dans le Règlement général sur la protection des données : *bis*

On notera encore que la loi-cadre impose la rédaction d'un protocole d'accord pour les autorités publiques fédérales qui envisagent un transfert de données à caractère personnel à destination d'une autre autorité publique ou d'un organisme privé[212].

Section 8

Responsabilité et recours

A. Le nouveau régime de responsabilité

Le R.G.P.D. innove sur le chapitre de la responsabilité, étant donné que son article 82 offre le choix d'intenter une action en responsabilité à l'encontre du responsable du traitement ou du sous-traitant[213]. Ce choix est en outre offert à toute personne et n'est donc pas réservé à la seule personne concernée. Des entreprises ou des pouvoirs publics pourraient aussi intenter une action en réparation[214].

L'objectif est d'assurer à tous la réparation de tout préjudice matériel ou immatériel causé par *un traitement illicite*. Il suffit en effet de démontrer qu'un préjudice résulte d'un traitement non conforme au R.G.P.D. (sans devoir prouver qu'il s'agit d'une faute[215]) pour que le responsable du traitement en soit tenu responsable.

La responsabilité du sous-traitant ne pourra être engagée que dans deux cas : lorsque celui-ci n'a pas respecté les instructions licites données par le responsable du traitement ou lorsqu'il n'a pas respecté les obligations que le R.G.P.D. met spécifiquement à sa charge[216]. Dès lors, pour engager la responsabilité du sous-traitant il faudra prouver, en plus du dommage et de la non-conformité au R.G.P.D., qu'il a commis un manquement à ses obligations légales ou contractuelles[217].

repetita placent?», in Law, Norms and Freedoms in cyberworld/Droit, Normes et Libertés dans le cybermonde, Bruxelles, Larcier, 2018, p. 609.

212 Art. 20 de la loi-cadre. Voy., sur ce point, la contribution d'Élise Degrave dans le présent ouvrage.

213 Pour une analyse complète de la question de la responsabilité, notamment la question de la compétence territoriale (excluant tout aménagement contractuel) et le fait que le R.G.P.D. n'autorise pas les clauses de limitation de responsabilité pour les dommages liés au traitement des données, voy. K. Rosier et A. Delforge, «Le régime de la responsabilité civile du responsable du traitement et du sous-traitant dans le RGPD», *in* C. de Terwangne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, *op. cit.*, pp. 665-700.

214 *Ibid.*, p. 691 ; L. Gérard, «Le contrôle par les cours et tribunaux», *in* C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique – Manuel de base*, *op. cit.*, p. 159.

215 Voy. K. Rosier et A. Delforge, «Le régime de la responsabilité civile du responsable du traitement et du sous-traitant dans le RGPD», *op. cit.*, pp. 684 et s.

216 Art. 82, § 2, R.G.P.D.

217 K. Rosier et A. Delforge, «Le régime de la responsabilité civile du responsable du traitement et du sous-traitant dans le RGPD», *op. cit.*, pp. 682 et s.

Tant le responsable du traitement que le sous-traitant pourront s'exonérer de leur responsabilité s'ils démontrent que le dommage ne leur est nullement imputable[218].

B. La multiplication des recours

Plusieurs types de recours sont ouverts aux personnes concernées qui estiment que le traitement de leurs données s'effectue en violation du R.G.P.D. ou que leurs droits sont violés[219].

Premièrement, toute personne concernée peut introduire une réclamation auprès de l'autorité de contrôle de l'État membre dans lequel se trouve sa résidence principale, son lieu de travail ou dans lequel la violation du R.G.P.D. aurait été commise[220]. Une telle procédure pourra déboucher sur l'imposition par l'autorité de contrôle de mesures correctrices, voire d'importantes amendes administratives[221]. On notera que l'A.P.D. n'est pas compétente pour l'octroi de dommages et intérêts[222]. En cas d'inaction de l'autorité de contrôle dans un délai de trois mois ou de désaccord avec une décision juridiquement contraignante prononcée par l'autorité de contrôle, la personne concernée peut introduire un recours devant les juridictions de l'État membre sur le territoire duquel l'autorité de contrôle est établie[223]. En Belgique, un recours contre les décisions de la chambre contentieuse de l'A.P.D., par exemple, en cas de contestation de l'amende administrative infligée, peut être introduit devant la Cour des marchés[224]. On regrettera, avec Élise Degrave[225], que ce recours soit organisé devant une cour spécialisée en matière financière et de concurrence économique, alors que «la protection des données est un des moyens visant à protéger les droits fondamentaux des citoyens»[226]. Le recours contre les autres décisions contraignantes que peut prendre l'A.P.D. se fait, quant à lui, devant le Conseil d'État, en application de l'article 14, § 1er, 1°, des lois coordonnées sur le Conseil d'État, du fait que l'A.P.D. peut être considérée comme une «autorité administrative indépendante»[227].

218 Art. 82, § 3, R.G.P.D.

219 Voy. L. Gérard, «Quatre types de recours pour un Règlement», *in* C. de Terwangne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, *op. cit.*, pp. 655 et s.

220 Art. 77, § 1er, R.G.P.D.

221 Mesures listées à l'article 58, § 2, du R.G.P.D. Voy. aussi l'article 221 de la loi-cadre.

222 L. Gérard, «Le contrôle par les cours et tribunaux», *op. cit.*, p. 159.

223 Art. 78 R.G.P.D.

224 Art. 108, § 2, de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données.

225 É. Degrave, «Le contrôle par l'autorité de protection des données», *in* C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique – Manuel de base*, *op. cit.*, pp. 152 et 153, et dans le présent ouvrage, «Le R.G.P.D., les lois belges et le secteur public».

226 É. Degrave, citée *in* projet de loi portant création de l'Autorité de protection des données, *Doc. parl.*, Ch. repr., 2017-2018, n° 54-2648/006, p. 50.

227 É. Degrave, «Le contrôle par l'autorité de protection des données», *op. cit.*, pp. 153 et 154.

Par ailleurs, divers recours sont ouverts devant des juridictions judiciaires : l'action en cessation devant le président du tribunal de première instance siégeant comme en référé[228] [229], l'action en réparation devant les tribunaux civils[230], et l'action devant le juge pénal. Ce dernier peut infliger une des sanctions pénales prévues aux articles 22 et suivants de la loi-cadre, punissant par exemple d'une amende de 250 à 15.000 euros certaines violations du R.G.P.D. ou de la loi-cadre effectuées par négligence grave ou avec intention malveillante, ou d'une amende de 100 à 20.000 euros « quiconque qui, pour contraindre une personne à lui donner son autorisation au traitement de données à caractère personnel la concernant, a usé à son égard de voies de fait, de violence ou menaces, de dons ou de promesses »[231].

Il appartient à la personne concernée de choisir la voie de recours qu'elle souhaite emprunter, la législation n'imposant pas de s'adresser d'abord à l'A.P.D. avant de saisir une juridiction. Afin d'éviter le cumul d'une sanction administrative et d'une sanction pénale, cumul qui violerait le principe *non bis in idem*, l'article 229 de la loi-cadre a prévu une procédure spécifique[232].

On soulignera que le R.G.P.D. a introduit la nouveauté que la personne concernée qui ne souhaite pas introduire elle-même sa réclamation ou son action en justice peut mandater un organisme, une organisation ou une A.S.B.L., dont les objectifs statutaires sont d'intérêt public et qui est actif/ve dans le domaine de la protection des droits et libertés des personnes concernées pour ce faire[233].

228 Art. 209 à 219 de la loi-cadre. Cette action vaut pour « tout traitement constituant une violation aux dispositions légales ou réglementaires concernant la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel » ainsi que pour 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, ou dont l'enregistrement, la communication ou la conservation sont interdits, au traitement de laquelle la personne concernée s'est opposée ou qui a été conservée au-delà de la période autorisée » (art. 209).

229 Pour déterminer le tribunal de première instance territorialement compétent, voy. L. Gérard, « Le contrôle par les cours et tribunaux », *op. cit.*, p. 158.

230 *Cf. supra*, pt A.

231 Art. 227, 3°, de la loi-cadre.

232 Voy. L. Gérard, « Le contrôle par les cours et tribunaux », *op. cit.*, p. 161.

233 Art. 80, § 1er, R.G.P.D.

Section 9
Flux transfrontières de données

Le R.G.P.D. ne révolutionne pas le régime des flux transfrontières de données, même s'il apporte d'intéressantes précisions et compléments[234]. Le chapitre V reprend les règles qui régissaient la matière depuis 1995 en intégrant les instruments légaux qui ont fait leur apparition depuis lors pour assurer une protection aux données qui franchissent les frontières de l'Union européenne. Ainsi, les transferts de données hors de l'espace de protection européen (c'est-à-dire hors de l'Union européenne et de l'Espace économique européen) sont interdits à moins que le pays de destination des données n'ait été reconnu comme assurant une protection adéquate aux données, ou que l'émetteur des données n'offre lui-même une protection adéquate par le biais de garanties appropriées telles des clauses contractuelles ou des règles d'entreprises contraignantes[235], ou enfin qu'une dérogation trouve à s'appliquer[236].

Pour ce qui concerne les transferts de données au sein de l'Union européenne, et plus largement dans l'Espace économique européen (E.E.E.), c'est le principe de la liberté de circulation des données à caractère personnel qui est l'objectif fondamental de l'adoption du R.G.P.D.[237]. Le choix d'un instrument juridique tel un règlement européen pour assurer la protection des données s'explique par cet objectif.

On regrettera que le législateur n'ait pas saisi l'occasion de l'élaboration du R.G.P.D. pour définir la notion de « transfert » qui aurait certes mérité une clarification[238]. Cette clarification peut au demeurant être trouvée dans la définition proposée par le Contrôleur européen de la protection des données (l'E.D.P.S.)

234 Pour de plus amples développements sur le régime des flux transfrontières de données, voy. C. de Terwangne et C. Gayrel, « Le R.GPD et les transferts internationaux de données à caractère personnel », *in* C. de Terwangne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, *op. cit.*, pp. 285 à 336 ; C. de Terwangne, « Chapitre 4. Quel régime pour les flux transfrontières de données ? », *in* C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique – Manuel de base*, *op. cit.*, pp. 105 et s.

235 Ces règles sont couramment évoquées sous leur appellation anglaise : *Binding Corporate Rules* (B.C.R.). Elles sont définies à l'article 4, 20°, du R.G.P.D.

236 Art. 44 et s. R.G.P.D. Les transferts qui ont lieu dans le cadre de la coopération entre autorités compétentes des États membres à des fins de prévention, de détection et de poursuite des infractions pénales, sont, quant à eux, encadrés par le titre 2 de la loi-cadre.

237 Art. 1er, § 1er, R.G.P.D.

238 Dans le même sens, voy. Contrôleur européen de la protection des données, avis du 7 mars 2012 sur le paquet de mesures pour une réforme de la protection des données, p. 21, pt 108, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_FR.pdf ; également C. Gayrel et R. Robert, « Proposition de règlement sur la protection des données – Premiers commentaires », *J.D.E.*, 2012, p. 179 ; C. Ponsart et R. Robert, « Le règlement européen de protection des données personnelles », *op. cit.*, p. 432.

dans son *position paper* sur la question des transferts de données. Le transfert est défini en ces termes : « la communication, la divulgation ou la mise à disposition de données à caractère personnel par un expéditeur relevant du règlement et conscient que le ou les destinataires y auront accès ou agissant dans cette intention »[239]. Dans le même sens, le Rapport explicatif de la Convention n° 108 du Conseil de l'Europe modernisée précise qu'« [u]n transfert de données intervient lorsque des données à caractère personnel sont communiquées ou mises à disposition d'un destinataire relevant de la juridiction d'un autre État ou d'une autre organisation internationale »[240].

Désormais, il n'appartiendra plus qu'à la Commission européenne de se prononcer sur le caractère adéquat du niveau de protection offert par un régime, que ce régime soit celui d'un pays tiers, d'un territoire ou d'un secteur dans un pays tiers, ou encore d'une organisation internationale.

Section 10
Rôle des autorités de contrôle et sanctions

Depuis vingt-cinq ans, la volonté d'une protection effective de l'individu passe par le biais de la création d'une ou plusieurs autorités de contrôle qui contribuent à la protection des droits et libertés de l'individu à l'égard du traitement des données. L'expérience acquise durant ces années a en effet démontré que lorsqu'elles sont dotées de compétences effectives et qu'elles jouissent d'une réelle indépendance dans l'exercice de leurs fonctions, de telles autorités sont devenues partie intégrante du système de contrôle de la protection des données dans une société démocratique.

En ce sens, on a vu que c'est essentiellement la multiplication des actions des autorités de contrôle nationales, notamment vis-à-vis de grandes entreprises d'outre-Atlantique, qui a fait progresser la protection des données sur le terrain de la visibilité, pas seulement dans les médias, mais également dans les prétoires. En témoigne le nombre exponentiel de décisions de la Cour de justice rendues en la matière depuis une dizaine d'années.

239 Contrôleur européen de la protection des données, « Le transfert de données à caractère personnel à des pays tiers et à des organisations internationales par les institutions et organes de l'Union européenne », Document d'orientation, 14 juillet 2014, p. 7, disponible à l'adresse https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_FR.pdf.

240 Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (S.T.E. n° 108), Rapport explicatif, adopté par le Comité des ministres du Conseil de l'Europe, à Elseneur, Danemark, le 18 mai 2018, § 101, disponible à https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4b.

L'article 57 du R.G.P.D. confie une impressionnante liste de vingt-deux missions aux autorités de contrôle tandis que l'article 58 leur attribue des pouvoirs accrus d'investigation et d'enquête, de décision et de sanction[241], d'autorisation et d'avis. Ces autorités disposent en outre du pouvoir d'ester en justice[242].

Un point mérite d'être particulièrement souligné parce qu'il a assuré à lui seul la publicité inédite qui a entouré l'adoption du R.G.P.D. : il s'agit du montant des amendes qui peuvent être prononcées à l'encontre des récalcitrants. Ces sanctions peuvent s'avérer extrêmement lourdes financièrement. Pour les manquements les plus graves, l'amende peut aller jusqu'à 20.000.000 euros ou, pour une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial de l'exercice précédent[243]. Cela donne irrémédiablement à réfléchir lorsqu'il est question de mettre en place un traitement de données à caractère personnel. C'est ce qu'auraient dû faire les entreprises Optical Center (punie d'une amende de 250.000 euros imposée par la CNIL)[244], Uber (qui a reçu une amende de £385.000 de la part de l'autorité britannique ICO[245]), Deutsche Wohnen S.E. (à qui l'autorité berlinoise a infligé une amende de 14,5 millions d'euros[246]), Google (sanctionnée d'une amende de 50 millions d'euros par la CNIL[247]) ou British Airways (qui a été prévenue de l'intention de l'ICO de lui infliger une amende de 183 millions de livres sterling – équivalant à 243,47 millions d'euros[248])[249]…

On ne peut manquer, à cet égard, de « s'interroger sur le principe même des sanctions extrêmement lourdes et se demander s'il est conciliable avec l'exigence de prévisibilité des règles à respecter. En effet, le respect du règlement appelle sur bien des points une appréciation au cas par cas et une pondération qui laisse à tout le moins place à la discussion »[250].

241 L'article 58, § 2, évoque des « mesures correctrices » allant depuis l'avertissement et le rappel à l'ordre jusqu'à l'amende ou la suspension.

242 Art. 58, § 5, R.G.P.D. Sur l'ensemble de ces missions et pouvoirs, voy. É. Degrave, « Le contrôle par l'Autorité de protection des données », *in* C. de Terwangne et É. Degrave, *La protection des données à caractère personnel en Belgique – Manuel de base*, *op. cit.*, pp. 146 et s.

243 Art. 83 R.G.P.D. Voy. également l'article 221 de la loi-cadre.

244 https://donnees-rgpd.fr/sanction/non-respect/.

245 https://ico.org.uk/action-weve-taken/enforcement/uber/.

246 https://fr.privacyvox.com/actualite/allemagne-sanction-de-145-me-pour-conservation-non-conforme-de-donnees/.

247 www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la.

248 www.timelex.eu/fr/blog/gdpr-amende-british-airways-societe-piratee-doublement-victime.

249 On relèvera qu'on est loin du montant de la sanction record prononcée par l'autorité américaine (la Federal Trade Commission) à l'encontre de Facebook le 24 juillet 2019 : 5 milliards de dollars…, www.lemonde.fr/pixels/article/2019/07/24/donnees-personnelles-les-États-unis-imposent-de-nouveaux-garde-fous-a-facebook-deja-contestes_5493017_4408996.html.

250 C. de Terwangne, K. Rosier et B. Losdijck, « Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel », *R.D.T.I.*, 2016, p. 57.

Conclusion

Devant les incessants développements techniques et dans le monde interconnecté qui est désormais le nôtre, la place de la législation de protection des données est passée inéluctablement à l'avant-plan. Le R.G.P.D. a l'ambition de combiner l'effectivité et la protection renforcée.

En décembre 2019, le Conseil de l'Union européenne a établi un premier bilan en vue de l'évaluation du R.G.P.D. qui doit être réalisée pour le 25 mai 2020, selon l'article 97 du texte. À cette occasion, le Conseil s'est montré enthousiaste : « *In the view of the Council, the GDPR has been a success. It is undoubtedly an important milestone and an instrument that strengthens the right to the protection of personal data and fosters trust-enabling innovation in the EU. The GDPR has also further increased awareness of the importance of data protection both in the EU and abroad* »[251].

Le Conseil n'a toutefois pas manqué de souligner le besoin de plus de précisions et d'orientations pratiques de la part des autorités de contrôle et du Comité européen de la protection des données[252]. Il a aussi relevé les divergences entre États membres qui sont apparues sur une série de points au travers des lois venues compléter le R.G.P.D. au niveau national. Les pages qui précèdent ont veillé à présenter la situation en Belgique, découlant de l'entrée en application du R.G.P.D. couplée à l'entrée en vigueur tant de la loi qui a instauré l'A.P.D. que de la loi-cadre du 30 juillet 2018.

La protection des données a indubitablement progressé depuis l'adoption de ces textes. Les droits des personnes concernées ont été singulièrement renforcés de même que la responsabilisation des différents acteurs. Les responsables de traitement ont vu apparaître des obligations de documentation interne, d'évaluation des risques, de dénonciation des incidents de sécurité, de nomination de personnel spécialisé… Et leur respect scrupuleux des règles de protection est vérifié par des autorités de contrôle aux pouvoirs remarquablement élargis. Les sanctions, surtout administratives, qui ont commencé à être prononcées par l'A.P.D. n'ont pas encore atteint les montants dissuasifs impressionnants réclamés par d'autres autorités de contrôle européennes, mais leur existence est déjà en soi un changement radical avec le passé en Belgique.

251 Council position and findings on the application of the General Data Protection Regulation (GDPR), Doc. 14994/1/19REV 1, 19 décembre 2019, https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/en/pdf, pt 9.

252 *Ibid.*, pt 12.