Les droits de la personne concernée dans le RGPD

Tombal, Thomas

Published in:
Le règlement général sur la protection des données (RGPD/GDPR)

Publication date:
2018

Document Version
le PDF de l'éditeur

TITRE 9
Les droits de la personne concernée dans le RGPD[1]

Thomas TOMBAL[2]

Introduction

1. Depuis l'adoption de la directive 95/46/CE[3] (ci-après « Directive »), les évolutions technologiques qu'ont connues nos sociétés ont été considérables. L'avènement des réseaux sociaux a ainsi profondément modifié nos rapports interpersonnels et notre conception du vivre ensemble. Étant toujours plus connectés, nous diffusons allègrement des informations nous concernant à qui le veut, qu'il s'agisse de proches ou d'inconnus vivant aux antipodes[4].

Il s'est donc avéré indispensable de mettre à jour les droits de la personne concernée, qui sont un des piliers de notre système européen de protection des données, en vue de rester en phase avec cette évolution.

---

[1] L'auteur remercie chaleureusement la professeure Cécile de Terwangne pour ses précieux conseils et intuitions, pour les discussions passionnantes et enrichissantes que nous avons eues sur les problématiques juridiques traitées, et pour le temps considérable consacré à la relecture de la présente contribution. L'auteur souhaite également remercier le professeur Jean-Noël Colin pour son expertise quant aux questions d'ordre technique dont nous avons pu discuter.

[2] Thomas Tombal est Chercheur au Centre de Recherche Information, Droit et Société (CRIDS), de l'Université de Namur. Il est spécialisé en matière de protection des données à caractère personnel, d'E-gouvernement et de propriété intellectuelle. Il collabore présentement au projet de recherche interdisciplinaire « FLEXPUB : Une nouvelle génération de services publics flexibles – le cas des données géographiques », financé par le programme BRAIN-be (Belgian Research Action through Interdisciplinary Networks) de BELSPO.

[3] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, 23 novembre 1995, L 281/31.

[4] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), 25 janvier 2012, COM(2012) 11 final, p. 1.

Ces droits de la personne concernée, recensés au chapitre III du RGPD[5], ont subi un lifting tantôt léger, tantôt novateur, et nous verrons, dans les pages qui suivent, que le phénomène des réseaux sociaux a servi de toile de fond à nombre de réflexions, notamment pour la création d'un nouveau droit à la portabilité des données, qui risque de faire couler beaucoup d'encre dans les années à venir.

2. Similairement à l'article 2, paragraphe 1er, a), de la Directive, le règlement général sur la protection des données[6] (ci-après « RGPD ») définit la personne concernée comme étant une « personne identifiée ou identifiable »[7]. Le RGPD est toutefois plus loquace que la Directive lorsqu'il s'agit de définir la notion de personne identifiable :

> « Est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence **à un identifiant**, **tel qu'un nom**, un numéro d'identification, **des données de localisation**, **un identifiant en ligne**, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, **génétique**, psychique, économique, culturelle ou sociale »[8] (nous soulignons).

Ceci résulte de la volonté claire du législateur européen de faire explicitement référence aux données génétiques des personnes physiques[9], ainsi qu'aux identifiants en ligne (tels que les adresses IP et les « cookies »[10]) et à d'autres types d'identifiants (citons ainsi les étiquettes RFID[11]), qui sont associés, par les équipements et les applications, aux utilisateurs de l'internet[12]. En effet, les traces du passage des utilisateurs, laissées par ces

---

[5] Art. 12 à 23 du RGPD.

[6] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, 4 mai 2016, L 119/1.

[7] Art. 4, § 1er, 1), du RGPD.

[8] Art. 4, § 1er, 1), du RGPD. Nous avons mis en évidence les ajouts par rapport à l'article 2, § 1er, a), de la Directive.

[9] Considérant n° 33 du RGPD. Notons que le RGPD définit les « données génétiques » comme étant « les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question » (art. 4, 13), du RGPD).

[10] Également connus sous le nom de « témoins de connexion ».

[11] « *Radio frequency identification tags* ».

[12] Considérant n° 30 du RGPD.

identifiants, permettent de profiler les personnes physiques auxquelles ils sont attribués[13].

3. Le décor ayant ainsi été brièvement planté, il s'agit maintenant de plonger dans l'analyse de ces droits contenus dans le RGPD.

Pour ce faire, nous allons, dans un premier temps, passer en revue l'ensemble des droits reconnus à la personne concernée, en mettant l'accent sur les modifications survenues par rapport à la Directive et sur les nouveautés apportées par le RGPD. Précisions d'emblée que l'une des particularités du RGPD est qu'il régit, en son article 12, les modalités d'exercice de l'ensemble des droits de la personne concernée. Cette disposition est en effet transversale, ce qui justifie, selon nous, qu'une section propre lui soit consacrée, au terme de l'analyse de chacun des droits de la personne concernée[14].

Dans un deuxième temps, nous étudierons le régime de la limitation de ces droits de la personne concernée, contenu à l'article 23 du RGPD.

[13] *Ibid.*

[14] Voy. chapitre 1, section 9, relative aux « Modalités de l'exercice des droits de la personne concernée (art. 12, §§ 2 à 6) ».

CHAPITRE 1. Les droits de la personne concernée

SECTION 1. – Droit d'être informée de l'existence de traitements la concernant

4. Afin de permettre à la personne concernée d'exercer ses droits, il est indispensable que celle-ci soit, d'abord et avant tout, informée, d'une part, du fait qu'un ou plusieurs responsable(s) de traitement traite(nt) des données à caractère personnel la concernant, et, d'autre part, de l'existence des droits qui lui sont reconnus par le RGPD.

Une lecture trop rapide de cet instrument pourrait laisser à penser que ce droit d'être informé est exhaustivement traité aux articles 12 à 14 du RGPD (§ 1). Or, il convient de préciser d'emblée que, dans certaines situations particulières, la personne concernée sera en droit d'obtenir des informations spécifiques, distinctes de celles contenues dans les articles susmentionnés (§ 2).

§ 1. Droit d'être informée du traitement

5. Avant de nous plonger dans l'étude de ce droit, pour la personne concernée, d'être informée du traitement dont elle fait l'objet, il convient de souligner une particularité organisationnelle dans la rédaction du RGPD. Ainsi, bien que les articles 12 à 14 soient contenus dans le chapitre du RGPD relatif aux droits de la personne concernée[15], ces articles sont formulés en termes d'obligations imposées au responsable de traitement. Certes, il s'agit là de deux revers d'une seule et même médaille, mais l'on peut se demander s'il n'eut pas été plus cohérent de formuler ces dispositions en termes de droits accordés à la personne concernée.

Ce faisant, il a été décidé, dans le cadre de cet ouvrage, de nous aligner sur la table des matières du RGPD et de traiter de cette question de l'information sous l'angle des droits de la personne concernée, plutôt que sous l'angle des obligations imposées au responsable du traitement.

a) Le principe de transparence des informations et des communications (art. 12, § 1er et 12, § 7, du RGPD)

6. Signe d'une volonté claire de modernisation de la protection des données personnelles, le premier article du chapitre III du RGPD introduit une nouveauté par rapport à la Directive.

Ainsi, l'article 12 du RGPD accorde à la personne concernée le droit d'attendre du responsable de traitement que celui-ci prenne des mesures appropriées afin de lui fournir les informations listées aux articles 13 et 14 du RGPD, ainsi que pour procéder à toute communication relative aux autres droits de la personne concernée « d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples »[16].

7. Ce principe nouveau, dit « de transparence », fait ainsi écho, comme cela a été souligné dans l'exposé des motifs du projet de RGPD[17], à la résolution de Madrid sur des normes internationales de vie privée[18].

Le RGPD précise également, à l'égard de ce principe, que :

---

[15] Chapitre III du RGPD.

[16] Art. 12, § 1er, du RGPD.

[17] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données, 25 janvier 2012, COM(2012) 11 final, p. 9).

[18] Résolution de Madrid sur des normes internationales de vie privée, 4-6 novembre 2009, 31e Conférence des commissaires à la protection des données et à la vie privée.

> « [Celui-ci] exige que toute information et communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples »[19] ; et qu'il
> « vaut tout particulièrement dans des situations où la multiplication des acteurs et la complexité des technologies utilisées font en sorte qu'il est difficile pour la personne concernée de savoir et de comprendre si des données à caractère personnel la concernant sont collectées, par qui et à quelle fin, comme dans le cas de la publicité en ligne »[20].

Ce principe vise ainsi à renforcer le contrôle des personnes concernées sur les données personnelles les concernant, et à rendre les responsables de traitement « *accountable* »[21] en assurant une plus grande visibilité sur les traitements qu'ils réalisent[22].

8. Il convient d'être précis. Ce qui est « nouveau » n'est pas l'idée même de la transparence du responsable du traitement vis-à-vis de la personne concernée. En effet, on peut considérer que l'obligation d'information de la personne concernée, imposée par la Directive aux responsables du traitement[23], remplissait déjà une telle finalité de transparence. La nouveauté résulte ici des conditions de formes auxquelles sont soumises la fourniture des informations contenues aux articles 13 et 14 du RGPD et les communications relatives aux droits des personnes concernées[24].

Comme indiqué ci-dessus, ces informations et communications doivent être fournies « d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples »[25]. Cette fourniture se fera par écrit ou par d'autres moyens qui s'avèreraient plus appropriés, par exemple par voie électronique[26].

Il est même suggéré au responsable de traitement – sans toutefois qu'il s'agisse d'une obligation – d'adjoindre à ces informations des « icônes

---

[19] Considérant n° 39 du RGPD.

[20] Considérant n° 58 du RGPD.

[21] Faute de traduction satisfaisante en français, le choix a été posé de garder le terme anglais. Précisons cependant que l'« *accountability* » pourrait se traduire par « la capacité de rendre des comptes ».

[22] Groupe 29, Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, 11 April 2018, p. 5.

[23] Art. 10 et 11 de la Directive.

[24] D. DE BOT, « De uitvoering van de algemene verordening gegevensbescherming – enkele bemerkingen bij de Belgische context », *T.V.W.*, 2016/3, p. 221.

[25] Art. 12, § 1er, du RGPD.

[26] *Ibid.* Le considérant n° 58 du RGPD donne ainsi l'exemple de la fourniture d'informations par le biais d'un site internet.

normalisées », qui permettraient d'offrir « une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible du traitement prévu »[27]. Si d'aventure le responsable du traitement faisait le choix de présenter de telles icônes par la voie électronique, le RGPD prévoit que celles-ci devront être lisibles par machine[28]. De telles icônes permettraient de simplifier la lecture des nombreuses informations devant être fournies aux personnes concernées, mais il ne convient pas non plus de basculer dans l'extrême inverse, en remplaçant la fourniture « classique » des informations par des icônes normalisées[29]. Il s'agit plutôt de combiner les deux modes de communication.

Enfin, ajoutons que ces informations peuvent même être fournies par voie orale, pour autant que la personne concernée en fasse la demande, et à la condition que l'identité de la personne concernée soit démontrée par d'autres moyens[30].

9. Bien que la formulation de cet article 12, paragraphe 1er, soit relativement abstraite, il convient de souligner que le Groupe 29 a adopté des lignes directrices relatives à ce principe de transparence, contenant des éléments de précision sur les notions employées dans le RGPD[31]. Nous allons en extraire les principaux éléments, et renvoyons à ces lignes directrices pour le surplus.

1° Concise, transparente, compréhensible et aisément accessible

10. Selon le Groupe 29, la fourniture des informations de façon « claire et transparente » implique que celles-ci soit présentées de façon succincte, afin d'éviter la fatigue des lecteurs, et idéalement dans une section propre des conditions générales[32]. Cette fourniture doit également être « aisément accessible », ce qui suppose que la personne concernée ne devrait pas avoir à chercher les informations, et devrait pouvoir identifier immédiatement et facilement où celles-ci se trouvent[33].

Cette fourniture d'information sera « compréhensible » si elle peut être comprise par « un membre moyen du public visé »[34]. Néanmoins, le

---

[27] Art. 12, § 7, du RGPD.

[28] Art. 12, § 7, du RGPD.

[29] Groupe 29, Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, 11 April 2018, p. 25.

[30] Art. 12, § 1er, du RGPD.

[31] Groupe 29, Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, 11 April 2018, disponible sur http://ec.europa.eu/newsroom/article 29/item-detail.cfm?item_id=622227.

[32] *Ibid.*, p. 7.

[33] *Ibid.*, p. 8.

[34] *Ibid*, p. 7. Traduction libre de : « *an average member of the intended audience* ».

Groupe 29 invite les responsables de traitement à vérifier régulièrement que leur « public réel » ait le même niveau de compréhension que le « public cible » anticipé, et à adapter, le cas échéant, l'information[35]. Une telle évaluation peut s'avérer complexe à mettre en œuvre en pratique, et il eût été préférable de simplement préciser que l'information doit être compréhensible par un « citoyen lambda », afin de créer un standard commun. Cela dit, dans certains cas, comme lors du traitement de données relatives à des enfants, le niveau spécifique du public cible pourra être plus facilement pris en compte[36].

2° Termes clairs et simples

11. Pour le Groupe 29, cette exigence de clarté et de simplicité requiert que les informations soient fournies par le biais de phrases simples et concrètes, en évitant de recourir à des structures de phrases et à des expressions complexes[37]. Ainsi, l'utilisation de termes ambigus et sujets à interprétation, tels que « peut », « pourrait », « certaines », « souvent » ou « possible », devrait être évitée[38].

3° Par écrit ou par d'autres moyens

12. S'il est vrai que l'écrit semble être la solution « par défaut » de fourniture des informations, celles-ci peuvent également être fournies par d'autres moyens, notamment électroniques, tels que des « *privacy policies* » ou des pop-ups[39]. D'après le Groupe 29, il conviendra, pour le responsable de traitement, de s'assurer que cette fourniture soit la plus appropriée possible aux circonstances particulières de l'interaction avec la personne concernée[40]. De surcroit, celle-ci devra être active, en ce sens que la personne concernée ne devrait pas avoir à chercher elle-même ces informations[41]. De plus, l'entièreté de ces informations devraient être disponibles dans un seul lieu ou dans un document complet[42].

---

[35] *Ibid.*

[36] Voy. *infra*, pt 14.

[37] Groupe 29, Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, 11 April 2018, p. 8.

[38] *Ibid.*, p. 9.

[39] *Ibid.*, pp. 11-12.

[40] *Ibid.*, p. 12.

[41] *Ibid.*, p. 18. Pour des suggestions de moyens techniques afin d'effectuer cette fourniture active, voy. pp. 19 à 22 de ces lignes directrices.

[42] *Ibid.*, p. 11.

4° Les informations peuvent être fournies oralement

13. L'article 12, paragraphe 1er, du RGPD prévoit que les informations peuvent être fournies oralement, à condition que la personne concernée en fasse la demande, et que l'identité de celle-ci soit démontrée par d'autres moyens. Pour le Groupe 29, cette vérification de l'identité, préalable à la fourniture orale des informations, n'est exigée que pour la fourniture d'informations relatives à l'exercice des droits de la personne concernée visés aux article 15 à 22 et à l'article 34 du RGPD, et non pour la fourniture des informations visées aux article 13 et 14 du RGPD, car ces dernières doivent également être accessibles aux futurs utilisateurs, dont le responsable de traitement ne connait, *a fortiori*, pas encore l'identité[43]. Cette fourniture orale peut notamment être réalisée par le biais d'un enregistrement sonore automatisé, qui devrait pouvoir être réécouté *a posteriori*[44].

b) Un principe de transparence renforcé pour les enfants (art. 12, § 1er et cons. 58 du RGPD)

14. Le principe de transparence susmentionné se voit renforcé lorsque les informations à fournir sont destinées spécifiquement à un enfant[45].

Le législateur européen considère, en effet, que :

> « Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel. Cette protection spécifique devrait, notamment, s'appliquer à l'utilisation de données à caractère personnel relatives aux enfants à des fins de marketing ou de création de profils de personnalité ou d'utilisateur et à la collecte de données à caractère personnel relatives aux enfants lors de l'utilisation de services proposés directement à un enfant »[46].

Dès lors, toute information ou communication relative à un traitement qui les concerne devra être rédigée en des termes clairs, simples et aisément compréhensibles pour ces enfants[47]. Ainsi, le vocabulaire, le ton et le style de langage employé devront être adaptés à ce public spécifique[48]. Le Groupe 29 précise également que les enfants conservent leur droit à recevoir ces informations conformément au principe de transparence ren-

---

[43] *Ibid.*, p. 12.
[44] *Ibid.*, p. 13.
[45] Art. 12, § 1er, du RGPD.
[46] Considérant n° 38 du RGPD.
[47] Considérant n° 58 du RGPD.
[48] Groupe 29, Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, 11 April 2018, p. 10.

forcée, quand bien même leurs parents auraient-ils consentis au traitement, en application de l'article 8 du RGPD[49].

c) Les informations à fournir lorsque les données à caractère personnel sont collectées auprès de la personne concernée (art. 13 du RGPD)

15. Lorsque le responsable du traitement collecte les données à caractère personnel auprès de la personne concernée, l'article 13 du RGPD octroie à la personne concernée le droit d'obtenir un certain nombre d'informations, qui peuvent être classées en deux catégories. Ainsi, certaines de ces informations devront être communiquées en toutes circonstances[50], tandis que d'autres ne devront être fournies que si elles s'avèrent nécessaires pour garantir un traitement équitable[51] et transparent à l'égard de la personne concernée[52]. Précisons néanmoins que le Groupe 29 est d'avis que toutes les informations contenues dans cet article devront être fournies en tout état de cause, sans distinction de « statut »[53].

Le responsable de traitement doit prendre des mesures appropriées pour fournir ces informations[54], ce caractère approprié devant être évalué sur la base du produit ou service en cause, des équipements utilisés et de la nature des interactions avec les personnes concernées[55].

Par ailleurs, le responsable de traitement doit également prendre toutes les mesures appropriées pour communiquer aux personnes concernées les éventuels changements substantiels ou matériels[56] dans le contenu de ces informations, en s'assurant que celles-ci en prennent effectivement connaissance[57]. Selon le Groupe 29, il conviendra d'informer la personne concernée préalablement à ces changements, en mettant notamment

---

[49] *Ibid.*, pp. 10-11.

[50] Art. 13, § 1er, du RGPD.

[51] Notons que dans la version anglaise du RGPD, les termes employés sont « *fair and transparent processing* ». Nous soulignons ceci car, le mot « *fair/fairly* » est également employé dans la version anglaise lorsque le texte français du RGPD évoque un traitement « loyal » (voy. not. l'article 5, § 1er, a), du RGPD). Il nous semble donc que les termes « traitement équitable » et « traitement loyal » doivent, en réalité, se voir accorder la même portée, et ce, en dépit de la différence de vocabulaire employé.

[52] Art. 13, § 2, du RGPD.

[53] Groupe 29, Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, 11 April 2018, p. 14.

[54] Art. 12, § 1er, du RGPD.

[55] Groupe 29, Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, 11 April 2018, p. 14.

[56] Pour déterminer si des changements sont substantiels ou matériels, le Groupe 29 invite le responsable de traitement à tenir compte de facteurs tels que l'impact sur la personne concernée et leur aptitude à exercer leurs droits, ou encore le caractère inattendu des changements pour ces personnes (*ibid.*, pp. 16-17).

[57] *Ibid.*, pp. 16-17.

l'accent sur l'impact potentiel de ceux-ci pour la personne, afin de lui permettre d'envisager sereinement les conséquences de ces changements et d'éventuellement exercer les droits qui lui sont attribués par le RGPD[58].

16. Une partie des informations visées dans cet article 13 du RGPD étaient déjà épinglées par l'article 10 de la Directive. Il s'agit plus précisément des informations suivantes

Informations à communiquer en toutes circonstances	Information à communiquer si cela s'avère nécessaire pour garantir un traitement équitable et transparent
– L'*identité du responsable du traitement* et, le cas échéant, de son représentant[59] ; – Les *finalités du traitement* auquel sont destinées les données à caractère personnel[60] ; – Les *destinataires*[61] *ou les catégories de destinataires* des données à caractère personnel[62].	– Des informations sur la question de *savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel* ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les *conséquences éventuelles de la non-fourniture de ces données*[63] ; – L'existence du *droit de demander* au responsable du traitement *l'accès* aux données à caractère personnel *et la rectification* de celles-ci[64].

17. Force est toutefois de constater que ce droit, pour la personne concernée, d'être informée a été largement précisé lors de l'adoption du RGPD.

D'une part, à l'inverse de l'article 10 de la Directive qui ne contenait aucune indication quant au moment exact auquel les informations devaient être fournies à la personne concernée, l'article 13 du RGPD précise dorénavant que ces informations doivent être transmises « au moment où les données en question sont obtenues »[65]. Cette précision a le mérite de clarifier la situation et de renforcer la sécurité juridique.

D'autre part, de nouvelles informations ont été adjointes, dans l'article 13 du RGPD, à la liste préexistante de l'article 10 de la Directive. Il s'agit plus précisément des informations suivantes :

---

[58] *Ibid.*, p. 17.

[59] Art. 13, § 1er, a), du RGPD ; art. 10, al. 1er, a), de la Directive.

[60] Art. 13, § 1er, c), du RGPD ; art. 10, al. 1er, b), de la Directive.

[61] Destinataire : « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires » (art. 4, 9), du RGPD).

[62] Art. 13, § 1er, e), du RGPD ; art. 10, al. 1er, c), 1er tiret, de la Directive.

[63] Art. 13, § 2, e), du RGPD ; art. 10, al. 1er, c), 2e tiret, de la Directive.

[64] Art. 13, § 2, b), du RGPD ; art. 10, al. 1er, c), 3e tiret, de la Directive.

[65] Art. 13, §§ 1er et 2, du RGPD.

Informations à communiquer en toutes circonstances	Information à communiquer si cela s'avère nécessaire pour garantir un traitement équitable et transparent
– Les *coordonnées du responsable du traitement* et, le cas échéant, de son représentant[66] ; – Le cas échéant, les *coordonnées du délégué à la protection des données*[67] ; – La *base juridique* du traitement[68] ; – Lorsque le traitement est fondé sur l'article 6, paragraphe 1er, f), du RGPD, les *intérêts légitimes poursuivis* par le responsable du traitement ou par un tiers[69] ; – Le cas échéant, le fait que le responsable du traitement a l'*intention d'effectuer un transfert de données* à caractère personnel vers un pays tiers ou à une organisation internationale, et *l'existence ou l'absence d'une décision d'adéquation* rendue par la Commission concernant ce pays tiers ou cette organisation internationale, ou, dans le cas des transferts visés à l'article 46 ou 47, ou à l'article 49, paragraphe 1er, alinéa 2, du RGPD, la *référence aux garanties appropriées ou adaptées* et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition[70].	– La *durée de conservation* des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée[71] ; – *L'existence du droit de demander* au responsable du traitement *l'effacement* des données à caractère personnel, ou une *limitation* du traitement relatif à la personne concernée, ou du *droit de s'opposer* au traitement et du *droit à la portabilité* des données[72] ; – Lorsque le traitement est fondé sur l'article 6, paragraphe 1er, a), ou sur l'article 9, paragraphe 2, a), du RGPD, *l'existence du droit de retirer son consentement à tout moment*, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci[73] ; – Le *droit* d'introduire une *réclamation auprès d'une autorité de contrôle*[74] ; – *L'existence d'une prise de décision automatisée*, y compris un *profilage*[75], visée à l'article 22, paragraphes 1er et 4, du RGPD, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée[76].

Précisons toutefois que, s'il est vrai que la liste des informations contenues à l'article 13 du RGPD est plus étoffée que celle de l'article 10 de la Directive, il convient de ne pas perdre de vue que la liste de l'article 10 de

[66] Art. 13, § 1er, a), du RGPD.
[67] Art. 13, § 1er, b), du RGPD.
[68] Art. 13, § 1er, c), du RGPD.
[69] Art. 13, § 1er, d), du RGPD.
[70] Art. 13, § 1er, f), du RGPD.
[71] Art. 13, § 2, a), du RGPD.
[72] Art. 13, § 2, b), du RGPD.
[73] Art. 13, § 2, c), du RGPD.
[74] Art. 13, § 2, d), du RGPD.
[75] Profilage : « 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 » (art. 4, 4), du RGPD).
[76] Art. 13, § 2, f), du RGPD. Voy. égal. : Groupe 29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251 rev.01, 6 February 2018.

la Directive était conçue comme étant une liste « *a minima* »[77], tandis que l'article 13 du RGPD semble être envisagé comme étant une liste exhaustive[78]. Cette divergence traduit sans nul doute la volonté du législateur européen de renforcer la sécurité juridique et l'harmonisation du droit de la protection des données en Europe.

18. Par ailleurs, l'article 13, paragraphe 3, du RGPD contient également une nouveauté par rapport à l'article 10 de la Directive. Ainsi, ce paragraphe dispose que, dans l'hypothèse 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 collectées, il devra fournir, au préalable, à la personne concernée, des informations au sujet de cette autre finalité et toute autre information pertinente visée à l'article 13, paragraphe 2, du RGPD[79]. Cet article doit être lu de concert avec l'article 5, paragraphe 1er, b), du RGPD, en ce sens que le traitement ultérieur doit être compatible avec la finalité de traitement originaire, à moins d'être fondé sur le consentement de la personne concernée ou sur un texte légal[80]. Le responsable de traitement devra en conséquence indiquer en quoi le traitement ultérieur est, à ses yeux, compatible avec la finalité du traitement originaire[81]. Par ailleurs, il conviendra d'informer la personne concernée suffisamment tôt de cette volonté d'effectuer un traitement ultérieur, afin de lui permettre de prendre en considération le potentiel impact de ceci et d'éventuellement exercer les droits qui lui sont attribués par le RGPD[82].

19. Enfin, précisons que l'article 13, paragraphe 4, du RGPD dispose qu'il n'y a pas lieu de procéder à la démarche d'informer la personne concernée « lorsque, et dans la mesure où, la personne concernée dispose déjà de ces informations ». Cela n'est pas novateur et apparaissait déjà dans l'article 10 de la Directive. Notons toutefois que, en pareil cas, le principe d'« *accountability* » requiert du responsable de traitement qu'il puisse

[77] L'article 10 de la Directive dispose en effet que le responsable du traitement doit fournir « au moins les informations énumérées ci-dessous », ce qui laissait la possibilité pour les États membres de compléter cette liste dans leurs lois de transposition.

[78] Rien ne semble toutefois interdire aux États membres d'ajouter des informations supplémentaires à cette liste, par le biais de législations nationales.

[79] Art. 13, § 3, du RGPD.

[80] Art. 6, § 4, du RGPD.

[81] Groupe 29, Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, 11 April 2018, p. 24.

[82] *Ibid*.

démontrer que la personne concernée a déjà reçu toutes ces informations et qu'elles n'ont pas été modifiées ou ne sont pas devenues obsolètes[83].

d) Les informations à fournir lorsque les données n'ont pas été collectées auprès de la personne concernée (art. 14 du RGPD)

20. À la différence de l'article 13 du RGPD, l'article 14 du RGPD vise l'hypothèse dans laquelle les données n'ont pas été collectées directement auprès de la personne concernée, mais plutôt par le biais d'une source externe ou d'un tiers[84].

À nouveau, sont ici visées deux catégories d'informations, à savoir celles devant être communiquées en toutes circonstances[85], et celles devant être fournies uniquement si elles s'avèrent nécessaires pour garantir un traitement équitable[86] et transparent à l'égard de la personne concernée[87]. Le Groupe 29 est, toutefois, d'avis que toutes ces informations devront être fournies en tout état de cause, sans distinction de « statut »[88].

De même, le responsable de traitement doit prendre des mesures appropriées pour fournir ces informations[89], ce caractère approprié devant être évalué sur la base du produit ou service en cause, des équipements utilisés et de la nature des interactions avec les personnes concernées[90].

Par ailleurs, le responsable de traitement doit également prendre toutes les mesures appropriées pour communiquer aux personnes concernées les éventuels changements substantiels ou matériels[91] dans le contenu de ces informations, en s'assurant que celles-ci en prennent effectivement connaissance[92]. D'après le Groupe 29, il conviendra d'informer

---

[83] *Ibid.*, p. 27.

[84] B. Docquir, *General Data Protection Regulation 2016 : Quelles obligations prévoit le projet de règlement européen sur les données personnelles (GDPR) ?*, consulté le 10 janvier 2016 sur le site http://www.simontbraun.eu/images/GDPR_Note_Generale_SimontBraun_Janv_2016.pdf, p. 23.

[85] Art. 14, § 1er, du RGPD.

[86] Voy. *supra*, la note infrapaginale n° 49.

[87] Art. 14, § 2, du RGPD.

[88] Groupe 29, Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, 11 April 2018, p. 14.

[89] Art. 12, § 1er, du RGPD.

[90] Groupe 29, Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, 11 April 2018, p. 14.

[91] Pour déterminer si des changements sont substantiels ou matériels, le Groupe 29 invite le responsable de traitement à tenir compte de facteurs tels que l'impact sur la personne concernée et leur aptitude à exercer leurs droits, ou encore le caractère inattendu des changements pour ces personnes (*ibid.*, pp. 16-17).

[92] *Ibid.*, pp. 16-17.

la personne concernée préalablement à ces changements, en mettant notamment l'accent sur l'impact potentiel de ceux-ci pour la personne, afin de lui permettre d'envisager sereinement les conséquences de ces changements et d'éventuellement exercer les droits qui lui sont attribués par le RGPD[93].

21. Tout comme pour l'article 13 du RGPD, une partie des informations visées dans cet article 14 du RGPD étaient déjà épinglées par l'article correspondant de la Directive, à savoir l'article 11. Il s'agit plus précisément des informations suivantes :

Informations à communiquer en toutes circonstances	Information à communiquer si cela s'avère nécessaire pour garantir un traitement équitable et transparent
– L'*identité du responsable du traitement* et, le cas échéant, de son représentant[94] ; – Les *finalités du traitement* auquel sont destinées les données à caractère personnel[95] ; – Les *catégories de données* concernées[96] ; – Les *destinataires ou les catégories de destinataires* des données à caractère personnel[97].	– *L'existence du droit de demander* au responsable du traitement *l'accès* aux données à caractère personnel et la *rectification* de celles-ci[98].

À nouveau, ce droit pour la personne concernée d'être informée en cas de collecte indirecte a été étoffé dans le RGPD.

22. Tout d'abord, des précisions ont été apportées quant au moment exact auquel les informations doivent être fournies à la personne concernée. De fait, la Directive mentionnait simplement que l'information devait avoir lieu « dès l'enregistrement des données ou, si une communication de données à un tiers est envisagé, au plus tard lors de la communication des données »[99]. L'article 14 du RGPD envisage, quant à lui, non plus deux, mais trois hypothèses.

Ainsi, les informations devront, en principe, être fournies par le responsable du traitement dans un « délai raisonnable » après avoir obtenu les données à caractère personnel[100]. Afin de déterminer ce délai, qui ne pourra jamais être supérieur à un mois, il conviendra pour le responsable

[93] *Ibid.*, p. 17.
[94] Art. 14, § 1er, a), du RGPD ; art. 11, § 1er, a), de la Directive.
[95] Art. 14, § 1er, c), du RGPD ; art. 11, § 1er, b), de la Directive.
[96] Art. 14, § 1er, d), du RGPD ; art. 11, § 1er, c), 1er tiret, de la Directive.
[97] Art. 14, § 1er, e), du RGPD ; art. 11, § 1er, c), 2e tiret, de la Directive.
[98] Art. 14, § 2, c), du RGPD ; art. 11, § 1er, c), 3e tiret, de la Directive.
[99] Art. 11, § 1er, al. 1er, de la Directive.
[100] Art. 14, § 3, a), du RGPD.

du traitement d'avoir égard aux circonstances particulières dans lesquelles les données sont traitées[101].

Dans l'hypothèse où le responsable du traitement doit utiliser les données à des fins de communication avec la personne concernée, le RGPD précise que ces informations devront être fournies au plus tard au moment de la première communication à ladite personne[102]. D'après le Groupe 29, ceci n'évince pas pour autant le délai de principe d'un mois mentionné ci-dessus, de sorte que, dans l'hypothèse en cause, le responsable de traitement devra fournir les informations au moment de la première communication (si celle-ci a lieu moins d'un mois après avoir obtenu les données) ou au plus tard un mois après avoir obtenu les données[103].

Enfin, si le responsable du traitement envisage de communiquer les données[104] à un autre destinataire, les informations devront être fournies au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois à un autre destinataire[105]. À nouveau, le Groupe 29 est d'avis que ceci n'évince pas le délai de principe d'un mois, de sorte que, dans l'hypothèse en cause, le responsable de traitement devra fournir les informations au moment de la communication au tiers (si celle-ci a lieu moins d'un mois après avoir obtenu les données) ou au plus tard un mois après avoir obtenu les données[106].

23. Ensuite, de nouvelles informations ont été adjointes, dans l'article 14 du RGPD, à la liste préexistante de l'article 11 de la Directive. Il s'agit plus précisément des informations suivantes :

---

[101] Art. 14, § 3, a), du RGPD.

[102] Art. 14, § 3, b), du RGPD.

[103] Groupe 29, Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, 11 April 2018, p. 15.

[104] Le texte français du RGPD mentionne ici la communication « d'informations ». Il nous semble qu'il s'agit là d'une erreur de traduction. En effet, le texte anglais mentionne simplement une « *disclosure* » (communication), sans préciser s'il s'agit d'une communication d'informations ou de données. Selon nous, il eut mieux valu évoquer une communication « de données », à l'instar de la formulation retenue à l'article 11, paragraphe 1er, alinéa 1er, de la Directive, qui fait plus de sens.

[105] Art. 14, § 3, c), du RGPD.

[106] Groupe 29, Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, 11 April 2018, p. 16.

Informations à communiquer en toutes circonstances	Information à communiquer si cela s'avère nécessaire pour garantir un traitement équitable et transparent
– Les *coordonnées du responsable du traitement* et, le cas échéant, de son représentant[107] ; – Le cas échéant, les *coordonnées du délégué à la protection des données*[108] ; – La *base juridique* du traitement[109] ; – Le cas échéant, le fait que le responsable du traitement a l'*intention d'effectuer un transfert de données* à caractère personnel à un destinataire dans un pays tiers ou une organisation internationale, et *l'existence ou l'absence d'une décision d'adéquation* rendue par la Commission concernant ce pays tiers ou cette organisation internationale, ou, dans le cas des transferts visés à l'article 46 ou 47, ou à l'article 49, paragraphe 1er, alinéa 2, du RGPD, la *référence aux garanties appropriées ou adaptées* et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition[110].	– La *durée* pendant laquelle les *données* à caractère personnel *seront conservées* ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée[111] ; – Lorsque le traitement est fondé sur l'article 6, paragraphe 1er, f), du RGPD, les *intérêts légitimes* poursuivis par le responsable du traitement ou par un tiers[112] ; – *L'existence du droit de demander* au responsable du traitement *l'effacement* des données à caractère personnel, ou une *limitation* du traitement relatif à la personne concernée, ou du *droit de s'opposer* au traitement et du *droit à la portabilité* des données[113] ; – Lorsque le traitement est fondé sur l'article 6, paragraphe 1er, a), ou sur l'article 9, paragraphe 2, a), du RGPD, *l'existence du droit de retirer le consentement à tout moment*, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci[114] ; – Le *droit* d'introduire une *réclamation auprès d'une autorité de contrôle*[115] ; – La *source* d'où proviennent les *données* à caractère personnel et, le cas échéant, une *mention* indiquant qu'elles sont *issues ou non de sources accessibles au public*[116] ; – *L'existence d'une prise de décision automatisée*, y compris un *profilage*, visée à l'article 22, paragraphes 1er et 4, du RGPD, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée[117].

[107] Art. 14, § 1er, a), du RGPD.
[108] Art. 14, § 1er, b), du RGPD.
[109] Art. 14, § 1er, c), du RGPD.
[110] Art. 14, § 1er, f), du RGPD.
[111] Art. 14, § 2, a), du RGPD.
[112] Art. 14, § 2, b), du RGPD.
[113] Art. 14, § 2, c), du RGPD.
[114] Art. 14, § 2, d), du RGPD.
[115] Art. 14, § 2, e), du RGPD.
[116] Art. 14, § 2, f), du RGPD.
[117] Art. 14, § 2, g), du RGPD. Voy. égal. : Groupe 29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251 rev.01, 6 February 2018.

Dans la lignée de notre analyse de l'article 13 du RGPD, il convient de préciser que s'il est vrai que la liste des informations contenues à l'article 14 du RGPD est, une nouvelle fois, plus fournie que celle de l'article 11 de la Directive, il convient de ne pas perdre de vue que la liste de l'article 11 de la Directive était également conçue comme étant une liste « *a minima* »[118], tandis que l'article 14 du RGPD semble être, à nouveau, construit comme étant une liste exhaustive.

24. Autre nouveauté par rapport à la Directive, l'article 14, paragraphe 4, du RGPD dispose que, dans l'hypothèse 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, il devra fournir, au préalable, à la personne concernée, des informations au sujet de cette autre finalité et toute autre information pertinente visée à l'article 14, paragraphe 2, du RGPD[119]. Comme indiqué pour l'article 13, paragraphe 3, du RGPD, cet article doit être lu de concert avec l'article 5, paragraphe 1er, b), du RGPD, en ce sens que le traitement ultérieur doit être compatible avec la finalité de traitement originaire, à moins d'être fondé sur le consentement de la personne concernée ou sur un texte légal[120]. Le responsable de traitement devra en conséquence indiquer en quoi le traitement ultérieur est, à ses yeux, compatible avec la finalité du traitement originaire[121]. De plus, il conviendra d'informer la personne concernée suffisamment tôt de cette volonté d'effectuer un traitement ultérieur, afin de lui permettre de prendre en considération le potentiel impact de ceci et d'éventuellement exercer les droits qui lui sont attribués par le RGPD[122].

25. Enfin, il convient d'aborder brièvement la question des dérogations possibles à ce droit de la personne concernée d'être informée en cas de collecte indirecte. Ces dérogations doivent être interprétées et appliquées strictement[123].

D'une part, un certain nombre de dérogations déjà contenues dans la Directive ont été reprises dans le RGPD.

---

[118] L'article 11 de la directive dispose en effet que le responsable du traitement doit fournir « au moins les informations énumérées ci-dessous ».

[119] Art. 14, § 4, du RGPD.

[120] Art. 6, § 4, du RGPD.

[121] Groupe 29, Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, 11 April 2018, p. 24.

[122] *Ibid.*

[123] *Ibid.*, p. 28.

Ainsi, les informations susvisées ne devront pas être fournies dans l'hypothèse où la personne concernée en disposerait déjà[124].

Tel sera également le cas lorsque leur fourniture se révèlerait impossible ou exigerait des efforts disproportionnées (en particulier pour un traitement à des fins archivistiques, statistiques ou de recherche scientifique ou historique), ou dans la mesure où la fourniture serait susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement[125]. Ajoutons que, dans ces trois cas, le responsable du traitement sera tenu de prendre des mesures appropriées pour protéger les droits, libertés et intérêts légitimes de la personne concernée[126].

Concernant l'hypothèse de l'impossibilité, le Groupe 29 précise bien qu'il doit s'agir d'une impossibilité « absolue », et qu'il n'existe pas de « degrés d'impossibilité »[127]. Les facteurs causant cette impossibilité peuvent d'ailleurs disparaître avec le temps, auquel cas il conviendra de fournir les informations[128].

Pour ce qui est de l'hypothèse des efforts disproportionnés, le Groupe 29 met en garde les responsables de traitement contre le fait de se prévaloir de cette exception de façon routinière par souci de facilité[129]. Ainsi, le responsable de traitement devrait uniquement se prévaloir de cette exception après avoir effectué une balance entre l'effort que lui imposerait la fourniture de ces informations aux personnes concernées, d'une part, et l'impact et les conséquences qu'une absence de communication entrainerait pour ces personnes, d'autre part[130].

Concernant la troisième hypothèse visée par l'article 14, paragraphe 5, b), du RGPD, le responsable de traitement devra, pour pouvoir bénéficier de cette exception, démontrer que la fourniture des informations serait, à elle seule, susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement[131].

Enfin, ces informations ne devront pas être fournies lorsque le droit de l'Union ou d'un État membre prévoit expressément l'obtention ou la

---

[124] Art. 14, § 5, a), du RGPD ; art. 11, § 1er, al. 1er, de la Directive.

[125] Art. 14, § 5, b), du RGPD ; art. 11, § 2, de la Directive.

[126] Pour des exemples de telles mesures appropriées, voy. : Groupe 29, Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, 11 April 2018, p. 31, pt 64.

[127] Groupe 29, Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, 11 April 2018, p. 29.

[128] *Ibid.*

[129] *Ibid.*, p. 30.

[130] *Ibid.*, p. 31.

[131] *Ibid.*

communication des données à caractère personnel[132]. La législation en question doit être donc suffisamment précise sur la collecte ou la communication des données pour qu'en en prenant connaissance, les personnes concernées se rendent compte que leurs données font l'objet d'un traitement[133]. Notons que, parallèlement à la dérogation précédente, le droit de l'Union ou de l'État membre devra prévoir des mesures appropriées destinées à protéger les intérêts légitimes de la personne concernée[134]. En pareil cas, le responsable de traitement devra s'assurer qu'il respecte scrupuleusement la législation en cause[135].

D'autre part, le RGPD intègre une dérogation supplémentaire à celles contenues dans la Directive. De fait, les informations listées à l'article 14, paragraphes 1er et 2, du RGPD ne devront pas être fournies lorsque les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union ou d'un État membre, y compris une obligation légale de secret professionnel[136]. Dans ce cas, il conviendra pour le responsable de traitement de démontrer que cette obligation de respect du secret professionnel s'applique directement à lui, afin de justifier l'absence de communication des informations[137].

§ 2. Droit de recevoir des informations spécifiques dans des situations particulières

26. Outre le droit, pour la personne concernée, d'être informée du traitement dont elle fait l'objet, le RGPD accorde, de façon clairsemée, à la personne concernée, le droit de recevoir des informations spécifiques dans des situations particulières.

---

[132] Art. 14, § 5, c), du RGPD ; art. 11, § 2, de la Directive. Il est à noter que la disposition du RGPD stipule qu'il n'y a pas d'obligation de fournir des informations aux personnes concernées lorsque « l'obtention ou la communication des **informations** sont expressément prévues par le droit de l'Union ou le droit de l'État membre » (nous soulignons), alors qu'il aurait fallu écrire, comme dans la directive « si la législation prévoit expressément l'enregistrement ou la communication des **données** » (nous soulignons).

[133] C. DE TERWANGNE, « L'utilisation des nouvelles technologies par le secteur financier face au droit à la vie privée et à la protection des données », in *The increasing impact of human rights law on the financial world*, coll. Cahiers de AEDBF/EVBFR-Belgium, Limal, Anthemis, 2016, p. 112.

[134] Groupe 29, Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, 11 April 2018, p. 32.

[135] *Ibid.*

[136] Art. 14, § 5, d), du RGPD.

[137] Groupe 29, Guidelines on transparency under Regulation 2016/679, WP 260 rev.01, 11 April 2018, p. 33.

Par souci de simplification de la lecture du RGPD quant au droit pour la personne concernée de recevoir un certain nombre d'informations, nous avons pris l'initiative d'énumérer et d'analyser brièvement ces cas particuliers dans la présente section.

a) Traitements ne nécessitant pas l'identification de la personne concernée (art. 11, § 2, du RGPD)

27. En vertu de l'article 11 du RGPD, lorsque les finalités poursuivies par le responsable de traitement ne lui imposent pas ou plus d'identifier une personne concernée, celui-ci n'est pas tenu de traiter des informations supplémentaires pour identifier la personne concernée à la seule fin de respecter le RGPD[138].

Néanmoins, lorsque, dans pareil cas, le responsable du traitement est à même de démontrer qu'il n'est pas en mesure d'identifier la personne concernée, il doit, « si possible », en informer la personne concernée[139].

À première vue, cette obligation spécifique d'information semble bien curieuse. En effet, comment le responsable du traitement pourrait-il bien informer la personne concernée du fait qu'il n'est pas en mesure de l'identifier, puisque, par hypothèse, il lui est nécessaire d'identifier cette personne pour pouvoir l'informer ?

En réalité, s'il est vrai que le responsable de traitement ne sera ici pas en mesure d'informer « personnellement » les personnes concernées dont il traite les données, puisqu'il n'est pas en mesure de les identifier, cela n'empêche pas ce responsable de traitement d'informer « collectivement » toute personne concernée potentielle.

Citons ainsi l'exemple d'un magasin qui aurait placardé, sur sa porte d'entrée, une affiche indiquant aux clients que certaines de leurs données seront collectées si le Bluetooth de leur smartphone est activé. En effet, par hypothèse, le gérant du magasin sait qu'il est susceptible de collecter certaines données à caractère personnel de ses clients, mais il ne connaitra jamais l'identité des clients dont il collecte *in fine* les données.

Cette constatation s'inscrit dans la lignée du rapport explicatif de la Convention 108 modernisée[140], qui précise, dans sa section relative à l'insertion d'un nouvel article 8 relatif à la transparence des traitements[141], que

---

[138] Art. 11, § 1er, du RGPD.

[139] Art. 11, § 2, du RGPD.

[140] Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), adoptée à Elseneur (Danemark) les 17 et 18 mai 2018, CM/Inf(2018)15-final.

[141] Dont la teneur est très proche du nouvel article 12 du RGPD.

« le responsable du traitement peut utiliser tous les moyens disponibles, raisonnables et économiquement abordables pour informer les personnes concernées, de façon collective (par un site web ou une information publique) »[142].

28. Concluons en mettant en exergue une certaine ambigüité quant aux modalités d'exercice des droits de la personne concernée, dans l'hypothèse visée par cet article 11 du RGPD.

Ainsi, dans l'article 12 du RGPD, il est stipulé que, dans les cas visés à l'article 11, paragraphe 2, du RGPD, le responsable de traitement ne peut pas refuser de donner suite à la demande de la personne concernée d'exercer les droits que lui confèrent les articles 15 à 22 du RGPD, à moins que le responsable de traitement ne démontre qu'il n'est pas en mesure d'identifier la personne concernée[143].

Cette disposition, prise à elle seule, parait logique puisque, si le responsable de traitement n'est pas en mesure d'identifier la personne concernée, il ne lui est, *a priori*, pas possible de donner suite à la demande de cette personne qui désire exercer ses droits.

L'ambigüité quant aux modalités d'exercice des droits de la personne concernée résulte, en réalité, de la formulation de la dernière phrase de cet article 11, paragraphe 2, du RGPD, qui dispose que les articles 15 à 20 du RGPD ne seront pas applicables[144], sauf si la personne concernée, aux fins d'exercer les droits que lui confèrent ces dispositions, adopte une attitude proactive et fournit au responsable de traitement des informations complémentaires qui permettent de l'identifier[145].

Ces deux dispositions paraissent à première vue contradictoires. En effet, l'article 12, paragraphe 2, du RGPD dispose que, dans l'hypothèse visée par cet article 11 du RGPD, il doit être donné suite aux droits de la personne concernée « à moins que », tandis que l'article 11, paragraphe 2, dernière phrase du RGPD dispose que, dans cette même hypothèse, les droits de la personne concernée ne seront pas applicables « sauf si ».

À vrai dire, une lecture en deux temps de ces dispositions permet de dégager une solution.

---

[142] Rapport explicatif du Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) – Convention 108 modernisée, CM(2018)2-addfinal, pt 70.

[143] Art. 12, § 2, du RGPD.

[144] Droit d'accès (art. 15), droit de rectification (art. 16), droit à l'effacement (art. 17), droit à la limitation du traitement (art. 18), obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement (art. 19) et droit à la portabilité (art. 20).

[145] Art. 11, § 2, du RGPD.

Ainsi, il convient tout d'abord de prendre en considération l'article 12, paragraphe 2, du RGPD. Le principe est donc que, dans l'hypothèse visée par cet article 11 du RGPD, la personne concernée peut exercer les droits qui lui sont conférés par les articles 15 à 22 du RGPD, « à moins que » le responsable de traitement ne démontre qu'il n'est pas en mesure d'identifier la personne concernée.

C'est donc uniquement si le responsable de traitement est parvenu à démontrer qu'il n'est pas en mesure d'identifier la personne concernée que l'article 11, paragraphe 2, dernière phrase, du RGPD devra être envisagé. En pareil cas, les articles 15 à 20 du RGPD[146] ne seront pas applicables, et la personne concernée ne sera pas en mesure d'exercer ses droits, « sauf si » cette personne adopte une attitude proactive et fournit au responsable de traitement des informations complémentaires qui permettent de l'identifier.

b) Accord entre responsables conjoints du traitement (art. 26, §§ 2 et 3, du RGPD)

29. L'article 26 du RGPD a trait aux accords conclus entre responsables conjoints de traitement[147], ce qui est une nouveauté introduite par le RGPD. Ceux-ci doivent, par la voie d'un accord, définir de manière transparente leurs obligations respectives en vue de se conformer aux règles du RGPD, en accordant une attention particulière à l'exercice des droits de la personne concernée et à la façon dont ils assureront la communication des informations visées aux articles 13 et 14 du RGPD[148]. À cet égard, un

[146] Notons ici une incohérence avec l'article 12, paragraphe 2, du RGPD, qui vise également les articles 21 (droit d'opposition) et 22 (droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé) du RGPD. Qu'advient-il de ces deux droits si le responsable de traitement est parvenu à démontrer qu'il n'est pas en mesure d'identifier la personne concernée ? Selon nous, ils doivent se voir appliquer le même régime que les articles 15 à 20. En effet, il nous semble qu'il s'agisse ici d'une erreur pure et simple (présente également dans la version anglaise), puisque les conséquences d'une lecture détachée de chacun de ces textes sont incompatibles. De fait, l'article 12, paragraphe 2, *in fine* permet au responsable du traitement de contrer l'application des droits contenus aux articles 15 à 22, tandis que l'article 11, paragraphe 2, dernière phrase, semble indiquer que cette application n'est, en pareil cas, contrée que pour les articles 15 à 20, ce qui est incompatible.

[147] Seront réputés responsables conjoints de traitement : « deux responsables du traitement ou plus [qui] déterminent conjointement les finalités et les moyens du traitement » (art. 26, § 1er, du RGPD).

[148] Art. 26, § 1er, du RGPD.

point de contact unique pour la personne concernée peut être identifié dans cet accord[149].

Cet accord doit dûment refléter les relations respectives des responsables conjoints avec la personne concernée, et les grandes lignes de l'accord doivent être mises à la disposition de cette dernière[150]. Il s'agit donc bien ici d'une situation particulière dans laquelle la personne concernée a le droit de recevoir des informations spécifiques.

30. Le dernier paragraphe de cet article 26 vient toutefois fortement nuancer le propos des deux premiers paragraphes. De fait, il résulte de l'article 26, paragraphe 3, du RGPD que les dispositions de l'accord relatives à l'exercice des droits de la personne concernée ne seront pas opposables à cette dernière, dès lors qu'elle reste libre d'exercer ses droits à l'égard de, et contre, chacun des responsables conjoints de traitement, et ce indépendamment des termes de l'accord[151].

Au vu de la formulation de ce dernier paragraphe, on pourrait se questionner sur l'intérêt d'avoir précisé dans le paragraphe premier qu'une attention particulière devait être accordée à l'exercice des droits de la personne concernée, puisque ces dispositions seront nécessairement inopposables à la principale intéressée.

Cette incohérence dans le texte final du RGPD s'explique probablement par l'évolution qu'a connue cet article dans les travaux préparatoires. Ainsi, dans la proposition de règlement introduite par la Commission, l'article relatif aux responsables conjoints de traitement ne contenait qu'un seul paragraphe, équivalent peu ou prou au paragraphe premier de la version finale du RGPD[152]. Il n'était donc nullement question d'une quelconque inopposabilité de cet accord à la personne concernée.

Ces développements relatifs à l'inopposabilité de l'accord furent introduits dans le second projet de règlement, rédigé par la présidence du Conseil de l'Union européenne[153], dans un article 24, paragraphe 2, qui

[149] *Ibid.*

[150] Art. 26, § 2, du RGPD.

[151] Art. 26, § 2, du RGPD.

[152] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données, 25 janvier 2012, COM(2012) 11 final, p. 63, art. 24.

[153] Présidence du Conseil de l'Union européenne, Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données – Préparation d'une orientation générale, 11 juin 2015, 9565/15.

correspond à l'actuel article 26, paragraphe 3, du RGPD. Ce second projet contenait toutefois un paragraphe supplémentaire (art. 24, § 3), qui faisait exception à cette règle de l'inopposabilité « pour les cas où la personne concernée a été informée de façon transparente et non équivoque de l'identité du responsable parmi les responsables conjoints, sauf en cas de fraude à ses droits »[154].

Le fait que cette exception n'ait pas été reprise dans la version finale du RGPD explique ainsi l'incohérence susmentionnée. Notons toutefois que, s'il est loisible à la personne concernée, indépendamment des termes de l'accord, de s'adresser au responsable conjoint de son choix pour l'exercice de ses droits, rien n'empêche les responsables conjoints de respecter, en interne, les termes de leur accord.

Ainsi, si cet accord prévoit que le responsable A est désigné comme point de contact pour les personnes concernées et que c'est à lui qu'incombe la responsabilité de faire suite à l'exercice des droits de la personne concernée vis-à-vis du responsable A et du responsable B, on peut tout à fait imaginer que ce soit le responsable A qui, sur cette base, accomplisse le travail en interne, quand bien même la personne concernée se serait-elle adressée au responsable B plutôt qu'au point de contact du responsable A désigné dans l'accord.

c) Communication à la personne concernée d'une violation de données à caractère personnel (art. 34 du RGPD)

31. L'article 34 du RGPD a trait au droit de la personne concernée d'être informée d'une violation de données à caractère personnel la concernant. Ceci n'est pas à proprement parler une « nouveauté » introduite par le RGPD. En effet, s'il est vrai qu'une telle disposition n'existait pas dans la Directive, le RGPD a ici intégré le contenu de l'article 3 du règlement de la Commission concernant les mesures relatives à la notification des violations de données à caractère personnel[155].

Nous n'allons pas, dans la présente section, nous attarder longuement sur cette question des violations de données, dès lors que ce point fait l'objet de développements exhaustifs au Titre 8, Chapitre 9, du présent

[154] B. Docquir, *General Data Protection Regulation 2016 : Quelles obligations prévoit le projet de règlement européen sur les données personnelles (GDPR) ?*, consulté le 10 janvier 2016 sur le site http://www.simontbraun.eu/images/GDPR_Note_Generale_SimontBraun_Janv_2016.pdf, p. 25.

[155] Règlement (UE) 611/2013 de la Commission du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques, *J.O.U.E.*, 26 juin 2013, L 173/2.

ouvrage. Par ailleurs, nous invitons le lecteur à consulter les lignes directrices y relatives, adoptées par le Groupe 29[156].

Nous nous contenterons simplement ici de pointer que, dans l'hypothèse où une telle violation de données serait « susceptible d'engendrer un risque élevé[157] pour les droits et libertés d'une personne physique »[158], le responsable du traitement se devra d'informer, dans les meilleurs délais, la personne concernée de ladite violation[159].

Cette communication devra décrire, en des termes clairs et simples, la nature de la violation, et contenir au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d), du RGPD[160].

32. Le responsable de traitement pourra toutefois échapper à cette obligation de communication dans plusieurs hypothèses listées à l'article 34, paragraphe 3, du RGPD, que nous ne détaillerons pas ici[161].

33. Enfin, dans le cas où le responsable de traitement n'aurait pas encore communiqué à la personne concernée la violation de données la concernant, l'autorité de contrôle pourra, si elle estime que la violation est susceptible d'engendrer un risque élevé, exiger du responsable de traitement qu'il procède à ladite communication[162].

---

[156] Groupe 29, Guidelines on Personal data breach notification under Regulation 2016/679, WP 250 rev.01, 6 February 2018.

[157] Notons que la Convention 108 modernisée contient également une disposition analogue (article 7) dans laquelle il est fait référence non pas à un risque élevé, mais à un risque d'« atteinte grave ». Ces deux qualifications nous semblent être assimilables. Le rapport explicatif de la Convention 108 modernisée précise à ce propos que : « la révélation de données couvertes par le secret professionnel, ou susceptible d'entraîner un préjudice financier, une atteinte à la réputation ou des dommages corporels ou une humiliation, pourrait être jugée constitutive d'une atteinte "grave" » (Rapport explicatif du Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) – Convention 108 modernisée, CM(2018)2-addfinal, pt 64). Il devrait en être de même pour la définition d'un « risque élevé ».

[158] Art. 34, § 1er, du RGPD.

[159] *Ibid.*

[160] Art. 34, § 2, du RGPD. Il s'agit du nom et des coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues (art. 33, § 3, b)), de la description des conséquences probables de la violation de données à caractère personnel (art. 33, § 3, c)), et de la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives (art. 33, § 3, d)).

[161] Sur cette question, voy. le Titre 8, Chapitre 9, du présent ouvrage.

[162] Art. 34, § 4, du RGPD.

d) Flux transfrontière de données hors UE non fondé sur une décision d'adéquation, ne présentant pas de garanties appropriées et ne bénéficiant pas d'une dérogation pour des situations particulières (art. 49, § 1er, al. 2, du RGPD)

34. Lorsque le responsable de traitement réalise un flux transfrontière de données à caractère personnel hors de l'Union, et que ce transfert n'est pas fondé sur une décision d'adéquation[163], ne présente pas de garanties appropriées[164] et ne bénéficie pas d'une dérogation pour des situations particulières[165], ce transfert ne peut avoir lieu que si le responsable de traitement respecte les conditions de l'article 49, paragraphe 1er, alinéa 2, du RGPD. Cette hypothèse fait l'objet de développements au Titre 6, Chapitre 3, Section 3, § 3, du présent ouvrage, auxquels nous nous contentons simplement ici de renvoyer.

Dans une telle hypothèse, le responsable de traitement devra, en sus de la fourniture des informations listées aux articles 13 et 14 du RGPD, informer la personne concernée du transfert et des intérêts légitimes impérieux qu'il poursuit.

[163] Art. 45 du RGPD.
[164] Art. 46 du RGPD.
[165] Art. 49, § 1er, du RGPD.

SECTION 2. – Droit d'accès (art. 15 du RGPD)

§ 1. Portée du droit

35. Toute personne concernée se voit reconnaitre un droit d'accès à ses données à caractère personnel détenues par le responsable de traitement. Ce droit est intrinsèquement lié au droit à l'information, analysé ci-dessus, qui confère à la personne concernée le droit d'obtenir « passivement » toute une série d'informations. Le droit d'accès, à l'inverse, permet à la personne concernée d'obtenir un certain nombre d'informations si celle-ci adopte une attitude active et interpelle le responsable de traitement. Il a pour fonction de permettre à cette personne concernée de vérifier la licéité des traitements effectués par ce responsable de traitement[166].

Ainsi, en vertu du droit d'accès, la personne concernée a le droit d'obtenir, « à des intervalles raisonnables »[167], de la part du responsable de

[166] Considérant n° 63 du RGPD.
[167] *Ibid.*

traitement, la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées[168].

Si d'aventure des données à caractère personnel la concernant sont traitées, la personne concernée reçoit le droit d'accéder auxdites données[169], ainsi qu'aux informations visées aux points a) à h) de cet article 15, paragraphe 1er, du RGPD[170]. Notons d'emblée que si le responsable de traitement traite une grande quantité de données relatives à la personne concernée, il lui sera possible de demander à celle-ci de préciser sur quelles données ou quelles opérations de traitement sa demande porte, avant de lui fournir les informations en question[171].

36. Tout d'abord, la personne concernée a le droit d'obtenir des informations relatives aux finalités du traitement[172], aux catégories de données à caractère personnel concernées[173], et toute information disponible quant à la source des données lorsque celles-ci ne sont pas collectées auprès de la personne collectée[174], comme cela était déjà prévu dans la Directive[175].

37. Ensuite, similairement à la Directive[176], la personne concernée a le droit d'être informée des destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées[177].

---

168 Art. 15, § 1er, du RGPD. Tel était également déjà le cas dans la Directive (art. 12, a), 1er tiret).

169 À titre d'exemple, le considérant n° 63 du RGPD pointe le droit, pour la personne concernée, d'accéder à ses données de santé. Sont ainsi mentionnées « les données de leurs dossiers médicaux contenant des informations telles que des diagnostics, des résultats d'examens, des avis de médecins traitants et tout traitement ou intervention administrés ».

170 Art. 15, § 1er, du RGPD. Notons que cette liste est moins étoffée que la liste des informations devant être fournies au titre du droit à l'information (art. 13, §§ 1er et 2, du RGPD). De fait, si des informations relatives :

- le cas échéant, aux coordonnées du représentant et du délégué à la protection des données du responsable de traitement (art. 13, § 1er, a) et b)) ;
- à la base juridique du traitement (art. 13, § 1er, c)) ;
- aux intérêts légitimes poursuivis par le responsable de traitement ou par un tiers lorsque ce traitement est fondé sur l'article 6, § 1er, f) (art. 13, § 1er, d)) ;
- à l'existence du droit à la portabilité des données (art. 13, § 2, b)) ; et
- à l'existence du droit de retirer à tout moment son consentement lorsque le traitement est fondé sur l'article 6, § 1er, a) ou sur l'article 9, § 2, a) (art. 13, § 2, b)) ;

doivent être fournies en vertu de l'article 13 du RGPD, ces mêmes informations ne doivent pas être fournies à la personne concernée lorsque celle-ci fait usage de son droit d'accès.

171 Considérant n° 63 du RGPD.

172 Art. 15, § 1er, a), du RGPD.

173 Art. 15, § 1er, b), du RGPD.

174 Art. 15, § 1er, g), du RGPD.

175 Art. 12, a), 1er tiret, de la directive pour les finalités et les catégories de données ; art. 12, a), 2e tiret, de la Directive pour l'origine des données.

176 Art. 12, a), 1er tiret, de la Directive.

177 Art. 15, § 1er, c), du RGPD.

Le RGPD attire toutefois à présent l'attention sur la mention des destinataires qui sont établis dans des pays tiers à l'Union européenne ou qui sont des organisations internationales[178]. Ceci traduit une volonté claire, dans le RGPD, de renforcer l'information et l'accès de la personne concernée en matière de flux transfrontières, comme l'illustre notamment l'article 49, paragraphe 1er, alinéa 2, du RGPD, que nous avons évoqué *supra*[179].

Cette constatation transparait également dans le second paragraphe de cet article 15 du RGPD consacré au droit d'accès. De fait, cette disposition prévoit que :

> « Lorsque les données à caractère personnel sont transférées vers un pays tiers ou à une organisation internationale, la personne concernée a le droit d'être informée des garanties appropriées, en vertu de l'article 46, en ce qui concerne ce transfert »[180].

La personne concernée aura ainsi le droit, par exemple, d'être informée de l'existence et du contenu des règles d'entreprises contraignantes[181] auxquelles le responsable de traitement s'est assujetti afin de fournir de telles garanties appropriées[182].

38. Par ailleurs, la personne concernée dispose désormais également, par le biais du droit d'accès, du droit de recevoir des informations relatives, lorsque cela est possible, à la durée de conservation des données à caractère personnel envisagée ou, lorsque cela n'est pas possible, aux critères utilisés pour déterminer cette durée[183]. Ceci n'était pas couvert par le droit d'accès sous l'empire de la Directive.

39. De plus, la personne concernée a le droit d'obtenir des informations relatives à l'existence du droit de demander au responsable du traitement la rectification, l'effacement ou la limitation des données à caractère personnel qui la concernent, ou du droit de s'opposer à ce traitement[184].

Deux commentaires méritent d'être formulés à propos de cette disposition.

D'une part, cette disposition illustre bien que le droit d'accès est, en réalité, la porte d'entrée, voire même la condition préalable à l'exercice

178 *Ibid.*
179 Voy. *supra*, pt 34.
180 Art. 15, § 2, du RGPD.
181 Voy. art. 47 du RGPD.
182 Art. 46, § 2, b), du RGPD.
183 Art. 15, § 1er, d), du RGPD.
184 Art. 15, § 1er, e), du RGPD.

des autres droits de la personne concernée[185]. La Directive contenait d'ailleurs un seul article regroupant à la fois le droit d'accès, le droit de rectification, le droit à l'effacement et le droit de limitation[186] de la personne concernée[187]. Par souci de clarté, le RGPD contient désormais un article spécifique pour chacun de ces droits de la personne concernée[188].

D'autre part, il convient de mentionner que le droit pour la personne concernée d'obtenir des informations relatives à l'existence du droit de s'opposer au traitement était absent de l'article 12 de la Directive et a été ajouté dans le RGPD[189].

Soulignons qu'il est, *a contrario*, étrange que l'existence du droit à la portabilité des données ne soit pas mentionné dans cet article 15, paragraphe 1er, e), du RGPD alors qu'il est visé par l'article 13, paragraphe 2, b), du RGPD relatif au droit à l'information. En réalité, le droit à la portabilité des données n'était mentionné dans aucune des dispositions correspondantes de la première proposition de RGPD[190]. La référence à ce droit à la portabilité, dans l'article relatif au droit à l'information, fût tout d'abord introduite en germe dans la position adoptée par le Parlement en première lecture, sous les termes de « droit d'obtenir des données »[191], et fût ensuite formalisée explicitement dans la seconde proposition de RGPD[192]. En revanche, une telle référence ne fût jamais suggérée, dans les textes susmentionnés, pour la disposition relative au droit d'accès[193].

---

185 C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », note sous C.J.U.E., 22 décembre 2010, *R.D.T.I.*, n° 43, 2011, p. 77.

186 Qualifié antérieurement de droit au « verrouillage » des données dans la directive.

187 Art. 12 de la Directive.

188 Droit d'accès (art. 15), droit de rectification (art. 16), droit à l'effacement (art. 17) et droit à la limitation du traitement (art. 18).

189 Art. 15, § 1er, e), du RGPD.

190 Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données, 25 janvier 2012, COM(2012) 11 final, art. 14, § 1er, d) et 15, § 1er, e).

191 Résolution législative du Parlement européen sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), 12 mars 2014, COM(2012)0011 - C7-0025/2012 - 2012/0011(COD), art. 14, § 1er, d).

192 Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données – Préparation d'une orientation générale, Présidence du Conseil de l'Union européenne, 11 juin 2015, 9565/15, art. 13, § 1*bis*, e).

193 Voy. art. 15, § 1er, e), des travaux préparatoires mentionnés aux notes infrapaginales nos 185 et 186.

Il s'agit vraisemblablement là d'un oubli malheureux de la part du législateur européen, car nous ne voyons pas quelle serait la raison qui permettrait de justifier que l'information relative à l'existence du droit à la portabilité ne soit fournie que dans le cadre du droit à l'information, et non dans le cadre du droit d'accès.

40. Autre nouveauté du RGPD, la personne concernée dispose à présent du droit de recevoir, au titre du droit d'accès, des informations relatives au droit d'introduire une réclamation auprès d'une autorité de contrôle[194].

41. Enfin, les dernières informations que la personne concernée a le droit d'obtenir au titre de l'article 15, paragraphe 1er du RGPD ont trait à l'existence, ou non, d'une prise de décision automatisée[195], y compris un profilage[196]. Dans un tel cas, la personne concernée devra recevoir des informations utiles concernant la logique sous-jacente du traitement qui la concerne[197], « ainsi que l'importance et les conséquences prévues de ce traitement pour [sa personne] »[198].

La portée de cette seconde partie de phrase, qui est un ajout du RGPD, reste assez obscure. En effet, qu'entend-t-on par « l'importance » d'un traitement pour la personne concernée ? Selon nous, deux voies d'interprétation sont possibles.

Soit le terme « importance » fait référence au degré de gravité des conséquences de ce traitement automatisé pour la personne, et il eût alors mieux valu simplement mentionner les « conséquences prévues de ce traitement », afin d'éviter cette redondance.

Soit le terme « importance » fait référence à une perception plus subjective qu'a la personne concernée sur cette prise de décision automatisée. Ainsi, comme le souligne la professeur C. de Terwangne dans une analyse de la réforme de la Convention 108 :

> « Ce droit [de connaitre la logique sous-jacente du traitement] risque d'ailleurs bien de devenir un des droits clés contribuant largement à la transparence et dès lors à l'auto-détermination informationnelle des individus car il permet à ceux-ci non pas seulement de savoir ce qui se passe avec leurs données, mais bien **de comprendre** »[199] (souligné dans le texte original).

---

194 Art. 15, § 1er, f), du RGPD.

195 Voy. art. 22 qui sera analysé *infra*.

196 Art. 15, § 1er, h), du RGPD.

197 Tel était également déjà le cas dans la Directive (art. 12, a), 3e tiret).

198 Art. 15, § 1er, h), du RGPD.

199 C. DE TERWANGNE, « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère

Le mot « importance » pourrait alors être lu comme faisant référence à l'importance pour la personne concernée de ne pas simplement recevoir des informations utiles concernant la logique employée, mais également de comprendre cette logique et cette décision. Ainsi, la personne concernée pourrait « légitimement souhaiter connaître les critères qui ont joué et le poids accordé à chacun d'eux »[200] pour comprendre la décision prise de façon automatisée.

Cette seconde option a le mérite de recentrer le débat autour du droit à l'autodétermination informationnelle, qui est le fondement de ce droit, pour la personne concernée, de connaitre la logique sous-jacente de la décision automatisée dont elle fait l'objet.

§ 2. Droit d'obtenir une copie

42. L'apport majeur du RGPD concernant le droit d'accès de la personne concernée est à trouver au troisième paragraphe de l'article 15. De fait, il est maintenant explicitement stipulé que « le responsable du traitement fournit une *copie des données* à caractère personnel faisant l'objet du traitement »[201] (nous soulignons). Ceci devrait permettre de renforcer le contrôle des personnes concernées sur les données personnelles les concernant. On retrouve à nouveau ici une trace de la mise en avant du droit à l'autodétermination informationnelle dont le RGPD est emprunt.

Cette précision est bienvenue et met fin au débat qui existait sous l'empire de la Directive, dès lors que l'incertitude régnait quant à la question de savoir si le droit d'accès, tel que présenté à l'article 12 de la Directive, permettait implicitement à la personne concernée d'obtenir une copie des données à caractère personnel la concernant. Cet article 12 de la Directive prévoyait en effet que la personne concernée avait le droit d'obtenir « la communication, sous une forme intelligible, des données faisant l'objet du traitement »[202], certains voyant, en cette phrase, le fondement permettant à la personne concernée d'obtenir une copie de ses données, tandis que d'autres y voyait la référence à un droit, plus limité, à la consultation ou à la simple visualisation desdites données.

43. Cette controverse autour du droit pour la personne concernée d'obtenir une copie de ses données personnelles au titre du droit d'accès

personnel », in C. CASTETS-RENARD (dir.), *Quelle protection des données personnelles en Europe ?*, Bruxelles, Larcier, 2015, p. 107.

200 *Ibid.*, p. 106.

201 Art. 15, § 3, du RGPD.

202 Art. 12, a), 2e tiret, de la Directive.

a d'ailleurs été soumise à l'appréciation de la Cour de justice de l'Union européenne en 2014[203].

Dans ces affaires jointes, trois personnes concernées avaient introduit une demande de permis de résidence aux Pays-Bas et avaient requis, à la suite de la décision de l'autorité compétente, une copie de la « minute » dressée par l'officier du service néerlandais de l'immigration et de la naturalisation, contenant des données personnelles relatives aux personnes concernées et dans laquelle l'officier expliquait, par le biais d'une analyse juridique, les raisons pour lesquelles il estimait que le permis de résidence devait être accordé ou non[204].

La politique originelle du Ministre compétent était d'accorder la fourniture d'une copie de ces « minutes » aux personnes concernées, mais, suite à un changement de politique, la décision a été prise de fournir, non plus la copie de ces « minutes », mais plutôt un document contenant un résumé des données personnelles de la personne concernée contenues dans les « minutes », ainsi que des informations sur la source de ces données et sur les éventuels tiers auxquels ces informations auraient été divulguées[205].

Ce changement de politique suscita plusieurs questions préjudicielles relatives au droit d'accès, adressées à la Cour de justice de l'Union européenne, qui les reformula comme suit :

> « les juridictions de renvoi cherchent, en substance, à savoir si l'article 12, sous a), de la directive 95/46 et l'article 8, paragraphe 2, de la Charte doivent être interprétés en ce sens que le demandeur d'un titre de séjour dispose d'un droit d'accès aux données le concernant qui figurent dans la minute et, dans l'affirmative, si ce droit d'accès implique que les autorités compétentes doivent lui fournir une copie de cette minute ou s'il suffit qu'elles lui communiquent un aperçu complet desdites données sous une forme intelligible »[206].

La Cour commença par rappeler que la Directive :

> « laisse [aux États membres] le soin de déterminer **la forme matérielle concrète que cette communication doit prendre, pour autant que**

[203] C.J.U.E., 17 juillet 2014, *YS c. Minister voor Immigratie, Integratie en Asiel* et *Minister voor Immigratie, Integratie en Asiel c. M et S.*, aff. jointes C-141/12 et C-372/12.

[204] X. TRACOL, « Back to basics : The European Court of Justice further defined the concept of personal data and the scope of the right of data subjects to access it », *Computer Law & Security Review*, n° 31 (2015), pp. 112-113.

[205] *Ibid.*, p. 112 ; C.J.U.E., 17 juillet 2014, *YS c. Minister voor Immigratie*, aff. jointes C-141/12 et C-372/12, §§ 16 et 17.

[206] C.J.U.E., 17 juillet 2014, *YS c. Minister voor Immigratie*, aff. jointes C-141/12 et C-372/12, § 50.

celle-ci [soit] « intelligible », c'est-à-dire qu'elle permet à la personne concernée de **prendre connaissance de ces données et de vérifier que ces dernières sont exactes** et traitées de manière conforme à cette directive, afin que cette personne puisse, le cas échéant, exercer les [autres droits qui lui sont conférés par la directive] »[207] (nous soulignons).

Ce faisant, la Cour en a déduit que :

« dans la mesure où l'objectif poursuivi par ce droit d'accès peut être pleinement satisfait par une autre forme de communication, **la personne concernée ne saurait tenir** ni **de l'article 12, sous a), de la directive 95/46** ni de l'article 8, paragraphe 2, de la Charte **le droit d'obtenir une copie du document ou du fichier original dans lequel ces données figurent**. Afin de ne pas donner à la personne concernée l'accès à des informations autres que les données à caractère personnel la concernant, **celle-ci peut obtenir une copie du document ou du fichier original dans lequel ces autres informations ont été rendues illisibles** »[208] (nous soulignons).

Enfin, la Cour a précisé que :

« Pour qu'il soit satisfait à ce droit d'accès, il suffit que le demandeur du titre de séjour **soit mis en possession d'un aperçu complet de l'ensemble de ces données sous une forme intelligible**, c'est-à-dire une **forme permettant** à ce demandeur **de prendre connaissance de ces données et de vérifier que ces dernières sont exactes** et traitées de manière conforme à cette directive, **afin qu'il puisse, le cas échéant, exercer les droits** qui lui sont conférés par les articles 12, sous b) et c), 14, 22 et 23 de ladite directive »[209] (nous soulignons).

Cet arrêt relatif au droit d'accès sous l'empire de la Directive appelle à la formulation de deux commentaires.

44. Premièrement, la Cour considère que le droit d'accès dont la personne concernée peut se prévaloir en vertu de la Directive porte

[207] X. TRACOL, « Back to basics : The European Court of Justice further defined the concept of personal data and the scope of the right of data subjects to access it », *Computer Law & Security Review*, n° 31 (2015), p. 115 ; C.J.U.E., 17 juillet 2014, *YS c. Minister voor Immigratie*, aff. jointes C-141/12 et C-372/12, § 57.

[208] X. TRACOL, « Back to basics : The European Court of Justice further defined the concept of personal data and the scope of the right of data subjects to access it », *Computer Law & Security Review*, n° 31 (2015), p. 115 ; C.J.U.E., 17 juillet 2014, *YS c. Minister voor Immigratie*, aff. jointes C-141/12 et C-372/12, § 58.

[209] C.J.U.E., 17 juillet 2014, *YS c. Minister voor Immigratie*, aff. jointes C-141/12 et C-372/12, § 59.

uniquement sur ses données personnelles et non sur le document ou le fichier original contant ces données[210]. La Cour met ainsi en exergue le fait que ce qui était consacré par la Directive était un droit d'accès « aux données », et non « aux documents ». De fait, les documents en question peuvent contenir des informations autres que les données personnelles de la personne concernée, auxquelles cette dernière ne peut avoir accès. Ce faisant, la Cour précise que la personne concernée peut uniquement obtenir une copie du document ou du fichier original dans lequel ces autres informations ont été rendues illisibles[211].

Cette conclusion nous paraît transposable au régime du droit d'accès sous l'empire du RGPD. En effet, le RGPD consacre la possibilité pour la personne concernée d'obtenir une « **copie des données** à caractère personnel faisant l'objet du traitement »[212], mais ne précise aucunement si la personne concernée a le droit d'obtenir une copie du « document original » dans lequel ces données sont contenues. Par ailleurs, l'article 15, paragraphe 4, du RGPD dispose que « le droit d'obtenir une copie [...] ne porte pas atteinte aux droits et libertés d'autrui », sans pour autant préciser s'il est question d'une copie « des données » ou « du document original contenant ces données ».

Une lecture combinée de l'article 15 du RGPD et de l'arrêt exposé ci-dessus nous parait donc bienvenue, afin de conclure que s'il est vrai que la personne concernée a le droit d'obtenir une copie « des données »[213], ceci n'emporte pas le droit pour cette personne d'obtenir une copie « du document original contenant ces données », puisque, dans certains cas, la communication de ce document original pourrait porter atteinte aux droits et libertés d'autrui[214], notamment au secret des affaires ou à la propriété intellectuelle[215]. Cependant, ces considérations relatives aux droits et libertés d'autrui ne devraient pas aboutir à refuser toute communication d'informations à la personne concernée[216].

45. Deuxièmement, nous sommes d'avis que cet arrêt de la C.J.U.E. ne permet, en revanche, pas d'affirmer que le droit d'obtenir une copie « des données », aujourd'hui consacré dans le RGPD, existait déjà de façon implicite sous l'empire de la Directive.

---

210 *Ibid.*, § 58.
211 *Ibid.*
212 Art. 15, § 3, du RGPD.
213 Art. 15, § 3, du RGPD.
214 Art. 15, § 4, du RGPD.
215 Considérant n° 63 du RGPD.
216 *Ibid.*

En effet, rappelons qu'antérieurement à cet arrêt, l'incertitude régnait quant à la portée concrète de l'article 12 de la Directive, celui-ci prévoyant simplement que la personne concernée avait le droit d'obtenir « la communication, sous une forme intelligible, des données faisant l'objet du traitement »[217]. Or, concrètement, la fourniture d'une copie des données n'était pas la panacée pour rencontrer cette exigence. De fait, la mise en place, par le responsable de traitement, de mesures techniques permettant la simple consultation ou visualisation desdites données aurait vraisemblablement pu être qualifiée de « communication des données sous une forme intelligible », puisqu'elle permettait de rencontrer l'objectif sous-jacent du droit d'accès, à savoir permettre à la personne concernée « de prendre connaissance de ces données et de vérifier que ces dernières sont exactes et traitées de manière conforme à cette directive, afin qu'il puisse, le cas échéant, exercer [ses autres] droits »[218].

La version française de l'arrêt susmentionné pouvait donner l'impression que la Cour avait mis fin à cette incertitude, puisqu'elle y indique que, « pour qu'il soit satisfait à ce droit d'accès, il suffit que [la personne concernée] soit **mise en possession** d'un aperçu complet de l'ensemble de ces données sous une forme intelligible »[219] (nous soulignons). Selon nous, on aurait pu y voir la consécration du droit d'obtenir une copie des données, puisque seule cette copie permet de mettre la personne concernée « en possession » des données. La simple consultation ou visualisation desdites données n'engendre, à l'inverse, pas cette « mise en possession ».

Toutefois, force est de constater que la même conclusion ne peut être atteinte à la lecture de la version anglaise et néerlandaise (langue usitée pour la procédure) de cet arrêt. En effet, le texte anglais est formulé comme suit « *it is sufficient for the applicant for a residence permit* ***to be provided with*** *a full summary of all of those data in an intelligible form* »[220] (nous soulignons), et la version néerlandaise comme suit : « *volstaat het dat aan de aanvrager van de verblijfstitel een volledig overzicht, in begrijpelijke vorm, van al deze gegevens* ***wordt gegeven*** »[221] (nous soulignons). Il est donc fait référence au fait de « fournir » les données dans la version anglaise, et au fait de « donner » les données dans la version néerlandaise, ce qui n'implique, selon nous, pas nécessairement une « mise en possession »,

[217] Art. 12, a), 2e tiret, de la Directive.
[218] C.J.U.E., 17 juillet 2014, *YS c. Minister voor Immigratie*, aff. jointes C-141/12 et C-372/12, § 59.
[219] *Ibid.*
[220] *Ibid.*
[221] *Ibid.*

l'accès aux données pouvant être « fourni » ou « donné » par le biais de la simple consultation ou visualisation desdites données.

Ajoutons, par ailleurs, que l'expression « aperçu complet de l'ensemble des données »[222] (« *a full summary of all of those data* » / « *een volledig overzicht van al deze gegevens* ») employée par la Cour était également empreinte d'insécurité juridique, dès lors qu'elle ne permettait pas de déduire si la Cour exigeait la communication, en des termes intelligibles, de l'ensemble des données personnelles, ou simplement d'un aperçu de ces données. De fait, l'expression « aperçu complet » (« *full summary* » / « *volledig overzicht* ») semble antinomique, car, *a fortiori*, un aperçu n'est forcément pas complet.

Fort heureusement, le RGPD est venu mettre un terme aux deux incertitudes subsistant suite à l'arrêt susmentionné de la Cour, puisque ce texte consacre dorénavant explicitement la possibilité pour la personne concernée d'obtenir une « **copie des données** à caractère personnel faisant l'objet du traitement »[223] (nous soulignons). Est donc à présent clairement reconnu le droit d'obtenir une copie de l'ensemble des données personnelles, et non un simple aperçu.

Soulignons, qu'une lecture isolée de l'article 15, paragraphe 3, du RGPD pourrait laisser à penser qu'il serait suffisant, pour le responsable de traitement, de fournir une copie brute de l'ensemble des données personnelles de la personne concernée. Si tel était le cas, la personne concernée recevrait bien souvent un amas de données totalement incompréhensibles pour elle. Ceci aurait représenté une régression non-négligeable par rapport au régime de protection de la Directive, dans laquelle l'article 12 relatif au droit d'accès prévoyait explicitement que les données devaient être communiquées « sous une forme intelligible ».

En réalité, il convient de rappeler que chaque article du RGPD relatif à un droit spécifique de la personne concernée doit être lu de concert avec l'article 12 du RGPD, relatif aux modalités de l'exercice de l'ensemble de ces droits. Or, cette disposition transversale prévoit que les données communiquées au titre des articles 15 à 22 du RGPD doivent l'être « d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples »[224]. Il n'est donc pas suffisant de fournir une copie des données. Encore faut-il traduire la signification de ces données en des termes clairs, simples et compréhensibles par toute personne, et non simplement par des experts ayant des compétences juridiques

[222] C.J.U.E., 17 juillet 2014, *YS c. Minister voor Immigratie*, aff. jointes C-141/12 et C-372/12, § 59.

[223] Art. 15, § 3, du RGPD.

[224] Art. 12, § 1er, du RGPD. Voy. égal. *supra*, pts 6 à 9.

ou informatiques. Le RGPD accentue ainsi formellement la nécessité de donner du sens aux données.

46. Enfin, précisons que, si l'exercice du droit d'accès est normalement gratuit, le responsable du traitement peut exiger le paiement de frais raisonnables basés sur les coûts administratifs[225] pour toute copie supplémentaire demandée par la personne concernée[226]. Par ailleurs, lorsque cette dernière choisit de présenter sa demande par voie électronique, les informations doivent être fournies sous une forme électronique d'usage courant, à moins que la personne concernée ne demande qu'il en soit autrement[227].

Notons également que, en vertu du considérant n° 63 du RGPD, le responsable du traitement devrait, lorsque cela est possible, pouvoir donner l'accès à distance à un système sécurisé permettant à la personne concernée d'accéder directement aux données à caractère personnel la concernant[228]. Cette recommandation a toutefois une portée limitée, au vu de sa formulation et du fait qu'elle n'a pas été reprise dans le texte de l'article 15 du RGPD.

§ 3. Articulation avec la limitation de la conservation des données à caractère personnel

47. Pour terminer nos développements relatifs au droit d'accès, il convient de dire quelques mots de l'articulation de ce droit avec l'obligation qu'a le responsable de traitement de limiter la conservation des données à caractère personnel à une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées[229].

Cette problématique est particulièrement pertinente lorsque la personne concernée désire avoir accès aux « *log files* »[230] du responsable de traitement, afin de déterminer quelles sont les personnes qui ont effectivement

---

[225] Sont ici uniquement visés, selon nous, les coûts de reproduction des données, et non le coût du salaire de la personne ayant cherché et rassemblé les données.

[226] Art. 15, § 3, du RGPD.

[227] Art. 15, § 3, du RGPD.

[228] Considérant n° 63 du RGPD. Citons ainsi, à titre d'exemple, la possibilité offerte aux citoyens belges d'accéder à distance et de façon sécurisée, via la carte d'identité électronique, à leur dossier au Registre national, afin notamment de prendre connaissance des entités ayant consulté leurs données lors des six derniers mois : http://www.ibz.rrn.fgov.be/fr/registre-national/mon-dossier/.

[229] Art. 5, § 1er, e), du RGPD.

[230] Journaux d'évènements conservant les « traces digitales » permettant d'identifier les accès concrets à des données à caractère personnel (C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », note sous C.J.U.E., 22 décembre 2010, *R.D.T.I.*, n° 43, 2011, p. 73).

eu accès aux – ou qui ont été les destinataires des – données à caractère personnel la concernant[231].

Comme le souligne la professeure C. de Terwangne, se pose en effet la question de savoir :

> « À partir de quand l'exercice du droit d'accès à des informations concernant le passé peut légitimement être paralysé par l'effacement de ces informations. Et pendant combien de temps les personnes détenant des données sont tenues de conserver les traces des actions passées effectuées sur ces données »[232].

48. Loin d'être simplement théorique, cette difficile articulation a fait l'objet d'une question préjudicielle posée à la Cour de justice de l'Union européenne[233]. Les faits à l'origine de cette affaire peuvent être résumés comme suit. Un citoyen néerlandais, M. Rijkeboer désirait obtenir de la part au Collège des bourgmestre et échevins de Rotterdam des informations relatives à toutes les instances dans lesquelles, au cours des deux années précédant sa demande, des informations le concernant avaient été transmises par l'administration communale à des tiers[234]. Ce dernier désirait plus particulièrement connaître l'identité des destinataires de ces données ainsi que le contenu des informations transmises[235]. Le Collège n'a toutefois pas été en mesure de donner entièrement suite à cette demande, dès lors qu'une loi néerlandaise[236] imposait l'effacement des données en cause à l'issue d'un délai d'un an[237].

Dans ce contexte, la question préjudicielle suivante fut posée à la Cour :

> « La limitation, prévue par la loi, de la communication des données à l'année précédant la demande concernée est-elle compatible avec l'article 12, [...] sous a), de la [directive], lue ou non en liaison avec

---

231 *Ibid.*

232 *Ibid.*

233 C.J.U.E., 7 mai 2009, *College van burgemeester en wethouders van Rotterdam c. m.e.e. Rijkeboer*, C-553/07.

234 C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », *op. cit.*, p. 74 ; C.J.U.E., 7 mai 2009, *Rijkeboer*, C-553/07, § 23.

235 C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », *op. cit.*, p. 74 ; C.J.U.E., 7 mai 2009, *Rijkeboer*, C-553/07, § 23.

236 Wet gemeentelijke basisadministratie persoonsgegevens, Stb. 1994, n° 494.

237 C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », *op. cit.*, p. 74 ; C.J.U.E., 7 mai 2009, *Rijkeboer*, C-553/07, §§ 24-25.

l'article 6, paragraphe 1, sous e), de cette directive et avec le principe de proportionnalité ? »[238].

Pour répondre à cette question, la Cour procéda en trois temps. Tout d'abord, elle a confirmé que :

« L'article 12, sous a), de la directive impose aux États membres de prévoir un droit d'accès à l'information sur les destinataires ou les catégories de destinataires des données ainsi qu'au contenu de l'information communiquée non seulement pour le présent, mais aussi pour le passé »[239].

De fait, comme le souligne, à juste titre, la Cour :

« Si tel n'était pas le cas, la personne intéressée ne serait pas en mesure d'exercer de manière efficace son droit de faire rectifier, effacer ou verrouiller les données présumées illicites ou incorrectes ainsi que d'introduire un recours juridictionnel et d'obtenir la réparation du préjudice subi »[240].

Ensuite, cette précision ayant été apportée, il était nécessaire pour la Cour de se pencher sur la question de la détermination du délai de conservation approprié des données en cause. Sur ce point, la Cour rappela d'emblée que s'il est vrai que les États membres disposent d'une certaine marge de manœuvre pour déterminer ce délai, celle-ci n'est pas illimitée[241]. De fait, comme le souligne la Cour :

« Il appartient aux États membres de fixer un délai de conservation de cette information ainsi qu'un accès corrélatif à celle-ci qui constituent un juste équilibre entre, d'une part, l'intérêt de la personne concernée à protéger sa vie privée, notamment au moyen des voies d'intervention et de recours prévus par la directive et, d'autre part, la charge que l'obligation de conserver cette information représente pour le responsable du traitement »[242].

Pour guider les États membres, la Cour a pointé un certain nombre de paramètres à prendre en considération, tels que le délai pour introduire un

---

238 C.J.U.E., 7 mai 2009, *Rijkeboer*, C-553/07, § 29.

239 C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », *op. cit.*, p. 78 ; C.J.U.E., 7 mai 2009, *Rijkeboer*, C-553/07, § 70.

240 C.J.U.E., 7 mai 2009, *Rijkeboer*, C-553/07, § 54.

241 C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », *op. cit.*, p. 79 ; C.J.U.E., 7 mai 2009, *Rijkeboer*, C-553/07, § 56.

242 C.J.U.E., 7 mai 2009, *Rijkeboer*, C-553/07, § 70.

recours, la nature plus ou moins sensible des données de base, la durée de conservation de ces données, le nombre des destinataires concernés[243] et la fréquence des communications[244]. Ces paramètres devront, bien évidemment, être mis en balance avec le souci de ne pas imposer d'obligations disproportionnées et de charges excessives, au responsable de traitement[245].

Enfin, la Cour a conclu, que, dans le cas d'espèce :

> « Une réglementation limitant la conservation de l'information sur les destinataires ou les catégories de destinataires des données et le contenu des données transmises à une durée d'un an et limitant corrélativement l'accès à cette information, alors que les données de base sont conservées beaucoup plus longtemps, ne saurait constituer un juste équilibre des intérêt et obligations en cause, à moins qu'il ne soit démontré qu'une conservation plus longue de cette information constituerait une charge excessive pour le responsable du traitement »[246].

49. Selon nous, le raisonnement que la Cour de justice de l'Union européenne a adopté, dans l'arrêt *Rijkeboer*, sur cette question de l'articulation entre droit d'accès et limitation de la conservation des données liées aux traces des accès des destinataires des données, devra également être suivi sous l'empire du RGPD.

§ 4. Exercice du droit

50. Particularité organisationnelle du RGPD, les modalités de l'exercice de ce droit d'accès ne sont pas contenues dans l'article 15 du RGPD relatif à ce droit, mais dans l'article 12, qui régit de façon commune les modalités d'exercice de l'ensemble des droits de la personne concernée[247].

Par souci d'économie de place, nous avons fait le choix de ne pas répéter lesdites modalités pour chacun des droits de la personne concernée, et nous invitons donc le lecteur à se référer à l'analyse de ces modalités que nous avons effectuée dans une section *ad hoc*[248].

---

[243] *Ibid.*, § 63.

[244] C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », *op. cit.*, p. 79 ; C.J.U.E., 7 mai 2009, *Rijkeboer*, C-553/07, § 59.

[245] *Ibid.*, p. 80 ; C.J.U.E., 7 mai 2009, *Rijkeboer*, C-553/07, §§ 59 et 60.

[246] C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », *op. cit.*, p. 80 ; C.J.U.E., 7 mai 2009, *Rijkeboer*, C-553/07, § 70.

[247] Voy. art. 12, §§ 2 à 6 du RGPD.

[248] Voy. chapitre 1, section 9, relative aux « Modalités de l'exercice des droits de la personne concernée (art. 12, §§ 2 à 6) ».

Précisons simplement, à ce stade, que cet article 12 dispose qu'une demande de la personne concernée relative à l'exercice du droit d'accès doit être traitée « dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande »[249], sauf exception[250]. De plus, à l'exception de la possibilité pour le responsable du traitement d'exiger le paiement de frais raisonnables pour toute copie supplémentaire de données personnelles la concernant demandée par la personne concernée[251], aucun paiement ne peut être exigé pour prendre toute mesure au titre du droit d'accès, à moins que la demande de la personne concernée ne s'avère manifestement infondée ou excessive[252].

[249] Art. 12, § 3, du RGPD.
[250] Pour plus de précisions sur cette question, voy. *infra*, pts 190 et 191.
[251] Art. 15, § 3, du RGPD.
[252] Art. 12, § 5, du RGPD. Pour plus de précisions sur cette question, voy. *infra*, pt 188.

SECTION 3. – Droit de rectification (art. 16 du RGPD)

§ 1. Portée du droit

51. Le droit de rectification permet à la personne concernée d'obtenir, dans les meilleurs délais, la correction des données à caractère personnel la concernant qui sont inexactes[253]. De même, elle a le droit d'exiger que les données à caractère personnel qui s'avèrent être incomplètes, compte tenu des finalités de traitement, soient complétées, le cas échéant en fournissant une déclaration complémentaire[254].

Ce droit était déjà contenu dans la Directive, plus précisément dans l'article 12 qui regroupait le droit d'accès, le droit de rectification, le droit à l'effacement et le droit de limitation de la personne concernée[255]. Il pouvait en effet paraitre justifié de traiter ces différents droits dans un seul et même article, dès lors que le droit d'accès est, comme nous l'avons souligné ci-dessus[256], la condition préalable à l'exercice des autres droits de la personne concernée[257].

Néanmoins, par souci de clarté, le RGPD contient désormais un article spécifique pour chacun des droits de la personne concernée, et donc un article 16 dédié exclusivement au droit de rectification.

---

[253] Art. 16 du RGPD.
[254] *Ibid.*
[255] Art. 12 de la Directive.
[256] Voy. *supra*, pt 39.
[257] C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », *op. cit.*, p. 77.

52. Il ne faut toutefois pas perdre de vue que cet article 16 du RGPD ne peut, à lui seul, permettre de comprendre la portée complète du droit de rectification.

En effet, comme le prévoyait déjà la Directive[258], ce droit de rectification s'accompagne d'un « droit de suite »[259], dont la teneur est contenue à l'article 19 du RGPD.

Ainsi, en vertu de ce « droit de suite », auquel il est fait référence sous le vocable « d'obligation de notification » dans le RGPD, le responsable du traitement est tenu de notifier, à chaque destinataire auquel les données à caractère personnel ont été communiquées, toute rectification effectuée conformément à l'article 16 du RGPD, à moins qu'une telle communication ne se révèle impossible ou exige des efforts disproportionnés dans le chef du responsable de traitement[260].

De surcroit, et à condition qu'elle en fasse la demande, la personne concernée a le droit de recevoir des informations relatives à ces destinataires[261]. Le RGPD est malheureusement muet quant aux informations concrètes qui doivent être fournies dans cette hypothèse. Selon nous, sont ici visées les informations qui devraient permettre à la personne concernée de vérifier que le responsable de traitement a bien « fait suivre » sa demande auprès de ces destinataires. Sont donc assurément visés l'identité et les coordonnées de ces destinataires. Le cas échéant, les coordonnées du délégué à la protection des données de ces destinataires pourraient également être pertinentes.

53. Le droit de rectification comporte donc un double volet, à savoir le droit d'obtenir la correction des données erronées, ainsi que le droit d'exiger que le responsable de traitement « fasse suivre » cette rectification en la notifiant aux destinataires desdites données à caractère personnel, sauf si cela exige des efforts disproportionnés.

En pratique, il est fort probable que des questions factuelles surgissent sur le caractère proportionné ou non de l'effort qui doit être fourni par le responsable de traitement afin de donner écho à ce droit de suite auprès de « chacun des destinataires ».

Il ne faut cependant pas perdre de vue qu'il est exigé du responsable de traitement que celui-ci tienne un registre renseignant notamment les catégories de destinataires auxquels les données à caractère personnel

---

[258] Voy. l'article 12, c), de la Directive.

[259] C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », *op. cit.*, p. 78.

[260] Art. 19 du RGPD ; art. 12, c), de la Directive.

[261] Art. 19 du RGPD.

ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales[262], et qu'il doit communiquer cette même information aux personnes concernées[263]. Ce faisant, nous sommes d'avis que, dans la majorité des cas, il ne sera pas considéré comme étant disproportionné de lui imposer l'effort supplémentaire que représente la notification de la rectification auprès de « chacun des destinataires ». En revanche, lorsque le traitement en cause consiste en une diffusion ou en une mise à disposition du public des données, exiger un droit de suite auprès de « chacun des destinataires » pourrait s'avérer être disproportionné. Pensons ainsi à la complexité, pour le responsable de traitement d'un site web tel que Wikipédia, Facebook ou Twitter, de relayer la correction d'une erreur présente sur ce site auprès de « chacun des destinataires ».

§ 2. Exercice du droit

54. Enfin, étant donné que les modalités de l'exercice de ce droit de rectification ne sont pas contenues dans l'article 16 du RGPD relatif à ce droit, mais dans l'article 12 du RGPD, qui régit de façon commune les modalités d'exercice de l'ensemble des droits de la personne concernée[264], nous invitons le lecteur à se référer à l'analyse de ces modalités effectuée *infra*[265].

Nous mettrons, ici, simplement en exergue que cet article 12 dispose qu'une demande de la personne concernée relative à l'exercice de ce droit doit être traitée « dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande »[266], sauf exception[267]. Par ailleurs, aucun paiement ne peut être exigé pour prendre toute mesure au titre du droit de rectification, à moins que la demande de la personne concernée ne s'avère manifestement infondée ou excessive[268].

---

262 Art. 30, § 1er, d), du RGPD.

263 Art. 13, § 1er, e) et f), du RGPD.

264 Voy. l'article 12, §§ 2 à 6, du RGPD.

265 Voy. chapitre 1, section 9, relative aux « Modalités d'exercice des droits de la personne concernée (art. 12, §§ 2 à 6) ».

266 Art. 12, § 3, du RGPD.

267 Pour plus de précisions sur cette question, voy. *infra*, pts 190 et 191.

268 Art. 12, § 5, du RGPD. Pour plus de précisions sur cette question, voy. *infra*, pt 188.

SECTION 4. – Droit à l'effacement (« droit à l'oubli ») (art. 17 du RGPD)

55. La disposition du RGPD relative au droit à l'effacement était, avec celle relative au droit à la portabilité que nous analyserons *infra*[269], sans aucun doute l'une des plus attendues par les acteurs de la protection des données.

En effet, s'il est vrai que le droit à l'effacement n'est, en tant que tel, pas nouveau dès lors qu'il était déjà prévu par la Directive[270], se posait toutefois la question de savoir comment ce droit allait s'articuler avec le concept nouveau de « droit à l'oubli », qui a fait l'objet de nombreuses contributions[271] suite au jugement rendu par la Cour de justice de l'Union européenne dans l'affaire *Google Spain*[272], sur lequel nous reviendrons brièvement pour entamer la présente section (§ 1).

De fait, nous verrons que, bien que ces deux droits soient cités côte à côte dans l'intitulé de l'article 17 du RGPD, ce qui pourrait laisser à penser qu'il ne s'agit là que de deux synonymes pour qualifier un même concept juridique, la portée de ces deux droits est, en réalité, d'après nous, distincte[273] (§§ 2 et 3).

---

[269] Voy. *infra*, chapitre 1, section 6, « Droit à la portabilité des données (art. 20 du RGPD) ».

[270] Art. 12, b), de la Directive ; C. Vande Vorst, « Algemene verordening gegevensbescherming : vijf nieuwigheden van dichterbij bekeken », *Cah. jur.*, 2016/4, p. 81.

[271] Voy. *inter alia*, C. Vande Vorst, « Algemene verordening gegevensbescherming : vijf nieuwigheden van dichterbij bekeken », *op. cit.*, pp. 75-85 ; C. Bartolini et L. Siry, « The right to be forgotten in the light of the consent of the data subject », *Computer Law & Security Review*, n° 32 (2016), pp. 218-237 (voy. plus particulièrement les nombreuses références citées en page 233, à la note de bas de page 123) ; 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 (dir.), *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, pp. 81-120 ; E. Defreyne et R. Robert, « L'arrêt "Google Spain" : une clarification de la responsabilité des moteurs de recherche … aux conséquences encore floues », note sous C.J.U.E. (GC), 13 mai 2014, C-131/12, *R.D.T.I.*, n° 54, 2014, pp. 53-114 ; Groupe 29, Guidelines on the implementation of the Court of Justice of the European Union judgement on « Google Spain and Inc v. Agencia Espanola de proteccion de datos (AEPD) and Mario Costeja Gonzalez » C-131/12, WP 225, 26 November 2014.

[272] C.J.U.E. (gde ch.), 13 mai 2014, *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, C-131/12.

[273] 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 », *op. cit.*, pp. 273-274.

56. Précisons, à cet égard, que les rédacteurs de la Convention 108 modernisée[274] ont opté pour la non-inclusion explicite d'un « droit à l'oubli » dans le texte révisé, estimant que les contours de ce nouveau droit étaient encore, à ce stade, trop flous et sujets à de vives discussions, de sorte qu'il était préférable de ne pas introduire de dispositions susceptibles de causer une atteinte disproportionnée aux droits fondamentaux concurrents que sont la liberté d'expression et d'information[275].

En effet, ces rédacteurs sont d'avis que la conjugaison des garanties existant par ailleurs, telles que la règle imposant l'effacement des données personnelles dont la conservation n'est plus nécessaire aux finalités pour lesquelles elles sont traitées[276] et les droits de rectification[277], d'opposition[278] et d'effacement[279] de la personne concernée, est suffisante pour appréhender le concept juridique de « droit à l'oubli »[280].

§ 1. L'arrêt *Google Spain* de la C.J.U.E.

57. Comme indiqué en guise d'introduction à la présente section, la décision de la Cour de justice de l'Union européenne dans l'affaire *Google Spain*[281] a suscité des remous considérables, la presse et le grand public y voyant notamment la création par la Cour du fameux « droit à l'oubli »[282].

58. Rappelons, tout d'abord, si tant est que de besoin, les faits pertinents de cette illustre affaire.

---

[274] Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), adoptée à Elseneur (Danemark) les 17 et 18 mai 2018, CM/Inf(2018)15-final.

[275] C. DE TERWANGNE, « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », *op. cit.*, p. 103.

[276] Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), adoptée à Elseneur (Danemark) les 17 et 18 mai 2018, CM/Inf(2018)15-final ; art. 5, § 1er, e), du RGPD.

[277] Convention 108 modernisée, art. 8, § 1er, e) ; art. 16 du RGPD.

[278] Convention 108 modernisée, art. 8, § 1er, d) ; art. 21 du RGPD.

[279] Convention 108 modernisée, art. 8, § 1er, e) ; art. 17 du RGPD.

[280] C. DE TERWANGNE, « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », *op. cit.*, p. 103.

[281] C.J.U.E. (gde ch.), 13 mai 2014, *Google Spain SL et Google Inc.*, C-131/12.

[282] C. BARTOLINI et L. SIRY, « The right to be forgotten in the light of the consent of the data subject », *op. cit.*, p. 231.

Un citoyen espagnol, M. Costeja González[283], avait interpellé l'autorité de contrôle espagnole *(Agencia Española de Protección de Datos* [ci-après « AEPD »]) afin d'introduire une réclamation à l'encontre du quotidien *La Vanguardia* et de Google Spain et de Google Inc. (ci-après « Google »), se fondant sur le fait que, lorsque son nom était introduit dans « Google Search », l'internaute voyait apparaitre des liens vers deux pages du site web de *La Vanguardia*, sur lesquelles figurait une annonce, mentionnant le nom de l'intéressé, pour une vente aux enchères immobilière liée à une saisie pratiquée en recouvrement de dettes de sécurité sociale[284].

Par son action, M. Costeja González demandait, d'une part, à l'encontre de *La Vanguardia*, la suppression ou, à tout le moins, la modification desdites pages afin que ses données personnelles n'y apparaissent plus, et, d'autre part, à l'encontre de Google, la suppression ou, à tout le moins, l'occultation de ses données personnelles afin que les liens vers le site de *La Vanguardia* cessent d'apparaître dans les résultats de recherche fondés sur son nom[285].

L'AEPD a rejeté ladite réclamation à l'encontre de *La Vanguardia*, estimant que la publication par cette dernière des informations en cause était légalement justifiée, mais a fait droit à la réclamation à l'encontre de Google[286].

Mécontent, Google fit appel de cette décision devant « l'*Audiencia Nacional* », qui posa plusieurs questions préjudicielles à la Cour de justice de l'Union européenne[287], certaines portant sur la question de savoir si l'AEPD avait bien le pouvoir d'ordonner à un moteur de recherche tel que Google de « déréférencer » certaines pages web suite à une demande d'une personne concernée, alors même que les informations en cause avaient été légitimement publiées sur le site web d'origine[288].

59. Sur cette question spécifique, la Cour a jugé que :

> « l'exploitant d'un moteur de recherche est obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des

[283] Soulignons ici l'ironie de la situation puisque le nom de cette personne, qui avait initié ces démarches afin d'accroitre son anonymat sur internet, ainsi que son passé, sont maintenant largement diffusés suite à cet arrêt majeur de la Cour de justice de l'Union européenne.

[284] C.J.U.E. (gde ch.), 13 mai 2014, *Google Spain SL et Google Inc.*, C-131/12, § 14.

[285] *Ibid.*, § 15.

[286] C.J.U.E. (gde ch.), 13 mai 2014, *Google Spain SL et Google Inc.*, C-131/12, §§ 16-17.

[287] *Ibid.*, §§ 18-20.

[288] C. Bartolini et L. Siry, « The right to be forgotten in the light of the consent of the data subject », *op. cit.*, p. 231.

tiers et contenant des informations relatives à cette personne, également dans l'hypothèse où ce nom ou ces informations ne sont pas effacés préalablement ou simultanément de ces pages web, et ce, le cas échéant, même lorsque leur publication en elle-même sur lesdites pages est licite »[289].

La Cour a également précisé que :

« il convient [...] d'examiner si la personne concernée a un droit à ce que l'information en question relative à sa personne ne soit plus, au stade actuel, liée à son nom par une liste de résultats affichée à la suite d'une recherche effectuée à partir de son nom, sans pour autant que la constatation d'un tel droit présuppose que l'inclusion de l'information en question dans cette liste cause un préjudice à cette personne [...]. [L'intérêt de la personne concernée prévaut], en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt [du] public à accéder à ladite information lors d'une recherche portant sur le nom de cette personne. Cependant, tel ne serait pas le cas s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question »[290].

60. Comme souligné ci-dessus[291], la presse et le grand public y ont vu la consécration par la Cour d'un nouveau « droit à l'oubli »[292]. En réalité, il convient d'être plus nuancé, et de considérer que, en tout état de cause, la Cour n'a abordé ici qu'un seul aspect du « droit à l'oubli », à savoir le droit au déréférencement des résultats de moteurs de recherche[293]. De fait, comme nous le verrons *infra*[294], la portée réelle du « droit à l'oubli » s'avère être bien plus large que cette seule question du droit au déréférencement dont la Cour a eu à connaitre.

---

289 *Ibid.* ; C.J.U.E. (gde ch.), 13 mai 2014, *Google Spain SL et Google Inc.*, C-131/12, § 88.

290 *Ibid.* ; C.J.U.E. (gde ch.), 13 mai 2014, *Google Spain SL et Google Inc.*, C-131/12, § 99.

291 Voy. *supra*, pt 57.

292 C. Bartolini et L. Siry, « The right to be forgotten in the light of the consent of the data subject », *op. cit.*, p. 231.

293 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 », *op. cit.*, p. 246.

294 Voy. Chapitre 1, section 4, § 3.

61. Précisons par ailleurs que, selon C. Bartolini et L. Siry, cette décision de la Cour s'apparente, à vrai dire, plutôt à une mise en œuvre spécifique du droit d'opposition qu'à la consécration d'un nouveau « droit à l'oubli »[295].

Ainsi, selon ces auteurs, plusieurs indices[296] tendent à démontrer que la Cour a simplement eu à traiter d'un cas particulier d'application du droit d'opposition formulé à l'encontre d'un responsable de traitement (Google), qui n'est pas le responsable de traitement ayant originellement traité les données personnelles *(La Vanguardia)*, mais qui a, au contraire, fait un traitement secondaire desdites données[297].

De fait, pour ces auteurs, les conséquences de l'arrêt *Google Spain* pour le cas d'espèce, s'inscrivent dans la lignée des conséquences naturelles de l'exercice ciblé, par une personne concernée, de son droit d'opposition, dès lors que, *in casu*, seul Google se voyait contraint de ne plus traiter les données personnelles en cause, tandis qu'il était loisible à *La Vanguardia* de continuer de traiter ces données (en laissant la page problématique en ligne)[298].

62. Notons, de surcroit, que ce droit au déréférencement conduit néanmoins à l'effacement de certaines données. De fait, si ce droit au déréférencement n'a pas pour effet d'effacer les données « originaires » (les articles de *La Vanguardia*), il implique toutefois l'effacement des données « secondaires » (les résultats du moteur de recherche Google) renvoyant vers ces données « originaires ».

Le responsable de traitement auprès de qui la demande de déréférencement est introduite par la personne concernée devra donc bien effacer certaines données de sa base de données, à savoir les résultats associés à une recherche menée sur la base du nom de cette personne concernée.

63. Il est également intéressant de souligner que le Groupe 29 a adopté des lignes directrices relatives à l'implémentation de l'arrêt *Google Spain*, dans lesquelles sont listés toute une série de critères devant être pris en compte par les responsables de traitements lorsqu'ils sont confrontés à une telle demande de la part de personnes concernées[299].

---

[295] C. Bartolini et L. Siry, « The right to be forgotten in the light of the consent of the data subject », *op. cit.*, p. 231.

[296] Nous avons fait le choix de ne pas passer ces indices en revue ici et, ce faisant, nous invitons le lecteur désireux d'en savoir plus à consulter la page 232 de la contribution susvisée.

[297] C. Bartolini et L. Siry, « The right to be forgotten in the light of the consent of the data subject », *op. cit.*, p. 232.

[298] *Ibid.*

[299] Groupe 29, Guidelines on the implementation of the Court of Justice of the European Union judgement on « Google Spain and Inc v. Agencia Espanola de proteccion de datos (AEPD) and Mario Costeja Gonzalez » C-131/12, WP 225, 26 November 2014, voy. spéc. pp. 12-20.

Notons que le Groupe 29 a précisé dans ces lignes directrices que ce droit au déréférencement vise principalement les moteurs de recherche dits « généralistes », et n'est pas applicable aux moteurs de recherches ayant un champ d'action limité, tels que les moteurs de recherches internes d'un site web[300].

64. Concluons cette sous-section consacrée au droit au déréférencement en attirant l'attention du lecteur sur le fait que le Conseil d'État français – dans le cadre d'un recours introduit par Google contre une décision de la CNIL[301] lui infligeant une sanction de 100.000 € suite au refus exprimé par le géant américain de procéder à un déréférencement sur l'ensemble des extensions de son nom de domaine[302] –, a posé à la Cour de justice de l'Union européenne une série de questions préjudicielles relatives à l'implémentation de ce droit au déréférencement[303]. Ces questions sont les suivantes :

> « 1° Le « droit au déréférencement » tel qu'il a été consacré par la Cour de justice de l'Union européenne dans son arrêt du 13 mai 2014 sur le fondement des dispositions des articles 12, sous b), et 14, sous a), de la directive du 24 octobre 1995, doit-il être interprété en ce sens que l'exploitant d'un moteur de recherche est tenu, lorsqu'il fait droit à une demande de déréférencement, **d'opérer ce déréférencement sur l'ensemble des noms de domaine de son moteur de telle sorte que les liens litigieux n'apparaissent plus quel que soit le lieu à partir duquel la recherche lancée sur le nom du demandeur est effectuée**, y compris hors du champ d'application territorial de la directive du 24 octobre 1995 ?
> 2° En cas de réponse négative à cette première question, le « droit au déréférencement » tel que consacré par la Cour de justice de l'Union européenne dans son arrêt précité doit-il être interprété en ce sens **que l'exploitant d'un moteur de recherche est seulement tenu**, lorsqu'il

[300] Groupe 29, Guidelines on the implementation of the Court of Justice of the European Union judgement on « Google Spain and Inc v. Agencia Espanola de proteccion de datos (AEPD) and Mario Costeja Gonzalez » C-131/12, WP 225, 26 November 2014, p. 8 ; 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 », *op. cit.*, p. 254.

[301] Commission nationale de l'informatique et des libertés.

[302] Google considère, en l'espèce, être uniquement tenu au déréférencement sur le nom de domaine www.google.fr, et non sur ses autres extensions, par exemple www.google.com, www.google.be ou www.google.de.

[303] Communiqué de presse du Conseil d'État français, *Portée territoriale du droit au déréférencement*, 19 juillet 2017, disponible sur http://www.conseil-etat.fr/Actualites/Communiques/Portee-territoriale-du-droit-au-dereferencement.

fait droit à une demande de déréférencement, **de supprimer les liens litigieux des résultats affichés à la suite d'une recherche effectuée à partir du nom du demandeur sur le nom de domaine correspondant à l'État où la demande est réputée avoir été effectuée ou**, plus généralement, sur les noms de domaine du moteur de recherche qui correspondent **aux extensions nationales de ce moteur pour l'ensemble des États membres de l'Union européenne** ?

3° En outre, en complément de l'obligation évoquée au 2°, le « droit au déréférencement » tel que consacré par la Cour de justice de l'Union européenne dans son arrêt précité doit-[il] être interprété en ce sens que l'exploitant d'un moteur de recherche faisant droit à une demande de déréférencement est **tenu de supprimer, par la technique dite du « géo-blocage », depuis une adresse IP réputée localisée dans l'État de résidence du bénéficiaire du « droit au déréférencement », les résultats litigieux des recherches effectuées à partir de son nom, ou même, plus généralement, depuis une adresse IP réputée localisée dans l'un des États membres soumis à la directive du 24 octobre 1995, ce indépendamment du nom de domaine utilisé** par l'internaute qui effectue la recherche ? »[304] (nous soulignons).

Les réponses apportées par la Cour seront déterminantes pour l'implémentation concrète future de ce droit au déréférencement.

D'une part, la portée de ce droit au déréférencement serait fortement limitée si la demande devait être renouvelée pour chaque extension d'un même nom de domaine, plutôt qu'une seule fois pour l'ensemble des extensions de ce nom de domaine.

D'autre part, si cette conception des extensions multiples, prônée par Google, devait être avalisée par la Cour, se poserait alors inévitablement une question essentielle en termes de charge de la preuve. En pareil cas, incombera-t-il à la personne concernée de démontrer que sa demande est justifiée pour chacune des extensions supplémentaires pour lesquelles elle voudrait exercer son droit au déréférencement ? Ou, au contraire, devra-t-on considérer que la demande de déréférencement est, *a priori*, justifiée pour l'ensemble des extensions, auquel cas il reviendra au responsable de traitement de démontrer en quoi cette demande serait disproportionnée pour telle ou telle extension ? Il est également envisageable que la Cour établisse une série de critères, notamment linguistiques ou géographiques, sur la base desquels la charge de la preuve incomberait tantôt à la personne

[304] C.J.U.E., Demande de décision préjudicielle présentée par le Conseil d'État (France) le 21 août 2017 – *Google Inc. c. Commission nationale de l'informatique et des libertés (CNIL)*, affaire C-507/17.

concernée, tantôt au responsable de traitement. Ainsi, on pourrait imaginer que si la demande de déréférencement originaire porte sur une extension européenne, telle que www.google.be, la charge de la preuve incombe tantôt au responsable de traitement pour les autres extensions européennes (.fr, .de, .nl, .eu, etc.) ou les extensions « génériques » (.com, .org, etc.), tantôt à la personne concernée pour les extensions hors-UE (.us, .ru, .ca, etc.).

Pour toutes les raisons évoquées ci-dessus, cet arrêt devrait avoir un impact essentiel sur le droit au déréférencement.

§ 2. Le droit à l'effacement tel que consacré par l'article 17 du RGPD

a) Précision terminologique : droit à l'effacement *sensu stricto*, droit à l'effacement au sens large et « droit à l'oubli »

65. Au vu du séisme médiatique qu'a causé cet arrêt *Google Spain*, une certaine incertitude régnait autour de l'impact concret qu'aurait cet arrêt sur la modernisation du droit à l'effacement, déjà consacré par l'article 12, b), de la Directive, et sur la potentielle inclusion dans le RGPD d'une disposition spécifique relative au « droit à l'oubli ».

De façon assez malheureuse sur le plan terminologique, le législateur européen a fait référence au droit à l'effacement et au « droit à l'oubli » dans l'intitulé de l'article 17 du RGPD : « Droit à l'effacement ("droit à l'oubli") ». Ainsi, un lecteur non-averti, pourrait, du fait de cette présentation, penser que droit à l'effacement et « droit à l'oubli » sont deux synonymes pour qualifier un même concept juridique.

Or, il convient, selon nous, d'être plus nuancé, et il est nécessaire de distinguer trois concepts, à savoir le droit à l'effacement *sensu stricto*, le droit à l'effacement au sens large et le « droit à l'oubli ».

66. Dans notre conception terminologique, le droit à l'effacement *sensu stricto* est le reliquat du droit à l'effacement préalablement consacré par l'article 12, b), de la Directive. Sa portée est la plus limitée parmi les trois concepts envisagés, dès lors qu'il permet uniquement à la personne concernée de demander l'effacement des données à caractère personnel ayant fait l'objet d'un traitement illicite[305]. Ce droit à l'effacement *sensu stricto* est ainsi, selon nous, consacré à l'article 17, paragraphe 1er, d), du RGPD.

[305] 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 », *op. cit.*, p. 263.

67. Le droit à l'effacement *sensu stricto* ne doit donc pas être confondu avec le concept plus vaste de « droit à l'effacement au sens large », qui doit, selon nous, être compris comme étant le droit à l'effacement tel que consacré par l'article 17 du RGPD, dont le droit à l'effacement *sensu stricto* ne constitue qu'un des éléments. Nous analyserons la portée concrète de ce droit à l'effacement au sens large ci-dessous[306].

68. Enfin, il semble que le concept juridique ayant la portée la plus étendue parmi les trois est « le droit à l'oubli », qui doit être considéré comme englobant non seulement le droit à l'effacement au sens large, mais également le droit au déréférencement des résultats de moteurs de recherche, consacré par la Cour de justice de l'Union européenne dans son arrêt *Google Spain*[307]. Nous reviendrons sur ce « droit à l'oubli » *infra*[308].

b) Portée du droit à l'effacement au sens large, tel que consacré par l'article 17 du RGPD

69. Le RGPD est venu élargir la portée du droit à l'effacement tel qu'il existait déjà sous l'empire de la Directive[309], et prévoit ainsi que :

> « La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique :
> a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;
> b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, § 1er, a), ou à l'article 9, § 2, a), et il n'existe pas d'autre fondement juridique au traitement ;
> c) la personne concernée s'oppose au traitement en vertu de l'article 21, § 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, § 2 ;
> d) les données à caractère personnel ont fait l'objet d'un traitement illicite [droit à l'effacement *sensu stricto*][310] ;

[306] Voy. chapitre 1, section 4, § 2, b).
[307] C.J.U.E. (gde ch.), 13 mai 2014, *Google Spain SL et Google Inc.*, C-131/12.
[308] Voy. chapitre 1, section 4, § 3.
[309] Art. 12, b), de la Directive.
[310] Nous ajoutons.

e) les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis ;
f) les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, § 1er »[311].

70. Avant d'analyser brièvement les différentes facettes de ce droit à l'effacement au sens large, il convient de tenir une réflexion plus générale, sur la question de savoir ce que signifie le terme « effacement ».

De fait, si, abstraitement, ce concept d'effacement semble ne pas poser de problèmes, force est de constater que, en pratique, les choses ne seront pas toujours aussi claires qu'il n'y paraît[312].

D'une part, il ne sera pas toujours possible pour le responsable du traitement d'être certain, sur le plan informatique, que les données ont bien été effacées[313].

D'autre part, il parait légitime, au vu du principe d'« *accountability* »[314] nouvellement intégré dans le RGPD, que le responsable du traitement désire garder une trace des demandes d'effacement qu'il a reçues et des suites qu'il a données auxdites demandes, afin de pouvoir en attester devant une autorité de contrôle ou une juridiction[315]. Ceci implique, *de facto*, que le responsable de traitement devra traiter des nouvelles données personnelles, relatives à la demande d'effacement. Ainsi, par exemple, si une personne concernée demande l'effacement des données à caractère personnel la concernant, traitées à des fins de marketing direct, suite à l'exercice de son droit d'opposition[316], il serait judicieux pour le responsable de traitement de conserver les coordonnées de cette personne, afin d'éviter de la contacter à l'avenir[317]. La constitution de cette liste de demandes d'effacement devrait pouvoir être fondée sur l'article 6, paragraphe 1er, f), du RGPD, qui considère comme licite le traitement

311 Art. 17, § 1er, du RGPD.

312 C. Vande Vorst, « Algemene verordening gegevensbescherming : vijf nieuwigheden van dichterbij bekeken », *op. cit.*, p. 82.

313 *Ibid.*

314 Voy. *supra*, Titre 8, Chapitre 2.

315 C. Vande Vorst, « Algemene verordening gegevensbescherming : vijf nieuwigheden van dichterbij bekeken », *op. cit.*, p. 82.

316 Art. 17, § 1er, c) et 21, § 2, du RGPD. Voy. égal. *infra*, pts 78-79 et 175.

317 Citons, à titre d'exemple, la liste Robinson qui permet aux consommateurs d'exprimer leur souhait de ne plus recevoir de sollicitations commerciales de la part des entreprises qui sont membres de la BDMA (Belgian Direct Marketing Association), que ce soit par courrier ou par téléphone (http://www.robinsonlist.be/index_fr.htm).

nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement, qui prévalent sur les intérêts ou les libertés et droits fondamentaux de la personne concernée[318].

1° Les multiples facettes du droit à l'effacement au sens large

71. Il ressort de la formulation de l'article 17, paragraphe 1er, du RGPD que cet instrument européen fait référence, dans cette disposition, à un droit à l'effacement au sens large, recouvrant de multiples facettes, et n'étant pas uniquement limité au droit à l'effacement *sensu stricto* déjà consacré dans la Directive[319] (i). Sont ainsi également envisagés le droit à l'effacement comme conséquence automatique du principe de finalité (ii), le droit à l'effacement suite au retrait de consentement (iii), le droit à l'effacement suite à l'exercice du droit d'opposition (iv) et le droit à l'effacement des données collectées dans le cadre de l'offre directe de services de la société de l'information aux enfants (v).

Notons que le droit à l'effacement au sens large recouvre également l'hypothèse de l'effacement pour respecter une obligation légale prévue par le droit de l'Union ou de l'État membre auquel le responsable du traitement est soumis[320]. Cette hypothèse n'appelle pas de commentaires particuliers, ce qui explique qu'une sous-section spécifique ne lui ait pas été consacrée ci-après.

i. Droit à l'effacement « sensu stricto »

72. Le droit à l'effacement au sens large englobe tout d'abord, le droit à l'effacement *sensu stricto*, consacré à l'article 17, paragraphe 1er, d), du RGPD, qui est la retranscription du droit à l'effacement préalablement consacré par l'article 12, b), de la Directive.

Ce droit permet à la personne concernée de demander l'effacement des données à caractère personnel ayant fait l'objet d'un traitement illicite, en contravention des règles de protection établies par le RGPD[321].

Le droit à l'effacement *sensu stricto* se distingue, en ce sens, du droit d'opposition et du droit au retrait de consentement, également visés par le droit à l'effacement au sens large, dès lors que ces derniers permettent à la personne

[318] C. Vande Vorst, « Algemene verordening gegevensbescherming : vijf nieuwigheden van dichterbij bekeken », *op. cit.*, p. 82.

[319] Art. 12, b), de la Directive.

[320] Art. 17, § 1er, e), du RGPD.

[321] 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 », *op. cit.*, p. 263.

concernée d'agir à l'encontre de traitements licites de données à caractère personnel la concernant réalisés par le responsable de traitement[322].

73. La Directive était relativement laconique sur ce qu'il convenait d'entendre par un traitement illicite[323], et évoquait simplement le caractère incomplet ou inexact des données traitées[324]. Le RGPD est, pour sa part, totalement muet sur la question.

Fort heureusement, la Cour de justice de l'Union européenne a, par son arrêt *Google Spain*[325], apporté des éclaircissements sur cette notion de traitement illicite[326], qui sont, selon nous, parfaitement transposables à l'article 17, paragraphe 1er, d), du RGPD.

La Cour a ainsi, tout d'abord, indiqué qu'un traitement illicite pouvait résulter d'autres situations que celles dans lesquelles les données traitées étaient incomplètes ou inexactes, dès lors que l'article 12, b), de la Directive n'évoque ces cas qu'à titre d'exemples, et non de façon limitative, puisqu'il est fait usage de la conjonction « notamment »[327].

Etayant son propos, la Cour a précisé qu'un tel traitement illicite :

> « peut résulter non seulement du fait que ces données sont inexactes, mais, en particulier, aussi du fait qu'elles sont inadéquates, non pertinentes ou excessives au regard des finalités du traitement, qu'elles ne sont pas mises à jour ou qu'elles sont conservées pendant une durée excédant celle nécessaire, à moins que leur conservation s'impose à des fins historiques, statistiques ou scientifiques »[328].

La licéité du traitement sera donc fonction de la qualité des données, qui s'apprécie non seulement au regard des finalités poursuivies, mais également du temps écoulé depuis la collecte, puisqu'il est parfaitement envisageable que, eu égard aux circonstances particulières du cas d'espèce, des données qui étaient pertinentes à l'origine ne le seront plus à partir d'un certain point dans le temps, voire deviennent même excessives[329].

---

322 *Ibid.*

323 Qualifié de « non-conforme » dans la Directive.

324 Art. 12, b), de la Directive.

325 C.J.U.E. (gde ch.), 13 mai 2014, *Google Spain SL et Google Inc.*, C-131/12.

326 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 », *op. cit.*, p. 263.

327 *Ibid.*, p. 263 ; C.J.U.E. (gde ch.), 13 mai 2014, *Google Spain SL et Google Inc.*, C-131/12, § 70.

328 *Ibid.* ; C.J.U.E. (gde ch.), 13 mai 2014, *Google Spain SL et Google Inc.*, C-131/12, § 92.

329 *Ibid.*, p. 264 ; C.J.U.E. (gde ch.), 13 mai 2014, *Google Spain SL et Google Inc.*, C-131/12, § 93.

De fait, à partir d'un certain moment, le traitement de ces données pourrait engendrer une atteinte excessive aux droits de la personne concernée, par rapport à l'intérêt qu'il représente pour le responsable du traitement.

Concluons en soulignant qu'il résulte également de cet arrêt de la Cour que « le caractère non conforme d'un traitement de données peut aussi découler du non-respect des conditions de licéité énoncées à l'article 7 de la [directive] et portant sur les hypothèses de légitimation des traitements de données[330] »[331].

ii. Le droit à l'effacement comme conséquence automatique du principe de finalité

74. Le droit à l'effacement au sens large comprend ensuite un « droit à l'effacement comme conséquence automatique du principe de finalité », en vertu duquel le responsable de traitement doit effacer les données à caractère personnel qui ne sont plus nécessaires au regard des finalités pour lesquelles elles sont traitées[332]. Nous utilisons le qualificatif de « conséquence automatique », dès lors que la personne concernée ne doit, en principe, faire aucun effort pour requérir cet effacement[333].

De fait, en vertu de la combinaison des principes de finalité et de limitation de la conservation des données[334], le responsable de traitement n'est en droit de conserver les données que pour autant que cette conservation se justifie au regard de la finalité de traitement[335]. Par conséquent, dès l'instant où la finalité en cause a été remplie ou dès l'instant où les données personnelles ne sont plus nécessaires pour la poursuite de cette finalité, le responsable de traitement devra automatiquement effacer les données en cause, ou, à tout le moins, les anonymiser[336].

L'insertion de cet article 17, paragraphe 1er, a), dans le RGPD reconnait ainsi explicitement aux personnes concernées le droit de vérifier que le responsable de traitement a bien respecté cette règle[337].

---

330 Dorénavant contenues à l'article 6 du RGPD.

331 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 », *op. cit.*, p. 264 ; C.J.U.E. (gde ch.), 13 mai 2014, *Google Spain SL et Google Inc.*, C-131/12, § 70.

332 Art. 17, § 1er, a), du RGPD.

333 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 », *op. cit.*, p. 262.

334 Art. 5, § 1er, b) et e).

335 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 », *op. cit.*, p. 262.

336 *Ibid.*

337 *Ibid.*

iii. Droit à l'effacement suite au retrait de consentement

75. Est également englobé dans le concept de droit à l'effacement au sens large, le droit pour la personne concernée de demander l'effacement des données à caractère personnel qui étaient traitées par le responsable de traitement sur la base d'un consentement octroyé par cette personne, dans l'hypothèse où cette dernière a retiré son consentement et où il n'existe pas d'autre fondement juridique justifiant le traitement[338]. Est ainsi consacré le « droit au repentir et à changer d'avis »[339].

76. L'insertion de cette disposition est loin d'être anodine, dès lors que, avant l'adoption du RGPD, la Directive ne prévoyait pas explicitement la possibilité pour la personne concernée de retirer son consentement[340].

Était ainsi suscitée la question de savoir si, à considérer qu'un tel retrait soit possible, ce retrait de consentement devait être assimilé à une forme de révocation ayant un effet *ex tunc*, de sorte que toutes les données collectées sur la base de ce consentement devaient être effacées par le responsable de traitement, ou si, au contraire, ce retrait n'avait qu'un effet *ex nunc*, de sorte que le responsable de traitement ne pouvait certes plus réaliser de nouveaux traitements sur les données collectées préalablement sur cette base – à l'exception de la conservation desdites données, cette opération étant couverte par la notion de traitement[341] –, mais n'était néanmoins pas tenu de les effacer[342].

77. Le RGPD semble avoir mis un terme à ce débat, puisque, en sus de l'insertion d'un article 7, paragraphe 3, qui prévoit que la personne concernée a le droit de retirer son consentement à tout moment, l'article 17, paragraphe 1er, b), précise que celle-ci peut, postérieurement au retrait de son consentement, requérir du responsable de traitement que celui-ci efface les données à caractère personnel qui avaient été, jusque-là, traitées sur la base de ce consentement[343].

---

[338] Art. 17, § 1er, b), du RGPD.

[339] 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 », *op. cit.*, p. 256.

[340] C. BARTOLINI et L. SIRY, « The right to be forgotten in the light of the consent of the data subject », *Computer Law & Security Review*, n° 32 (2016), p. 227.

[341] Art. 4, 2), du RGPD.

[342] C. BARTOLINI et L. SIRY, « The right to be forgotten in the light of the consent of the data subject », *op. cit.*, p. 227.

[343] 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 », *op. cit.*, p. 256.

Au vu de l'articulation de ces deux dispositions, il semble donc que le débat susmentionné ait été tranché comme suit : le retrait de consentement, en tant que tel, effectué sur le fondement de l'article 7, paragraphe 3, du RGPD n'a qu'un effet *ex nunc*, et non *ex tunc*, puisqu'il n'implique pas *de facto* un effacement des données personnelles préalablement traitées sur la base de ce consentement. Cependant, il sera loisible à la personne concernée de demander, postérieurement au retrait de consentement, et sur la base de l'article 17, paragraphe 1er, b), du RGPD, l'effacement des données en cause.

iv. Droit à l'effacement suite à l'exercice du droit d'opposition

78. Le droit à l'effacement au sens large englobe, par ailleurs, le droit pour la personne concernée de demander l'effacement des données à caractère personnel au traitement desquelles elle s'est préalablement opposée avec succès en exerçant le droit d'opposition qui lui est octroyé par l'article 21 du RGPD[344].

Nous ne creuserons pas, à ce stade, les questions liées au droit d'opposition, dès lors que ce droit sera étudié dans une section ultérieure, à laquelle nous nous permettons ici de simplement faire renvoi[345].

79. Précisons toutefois que le droit d'opposition se distingue du droit de retirer son consentement, mentionné précédemment[346], sur deux plans.

D'une part, le droit de retirer son consentement ne pourra, par hypothèse, être exercé que dans les cas où le traitement est fondé sur le consentement de la personne concernée, tandis que l'exercice du droit d'opposition ne couvre pas cette hypothèse[347].

D'autre part, la personne concernée ne doit pas justifier le retrait de son consentement tandis que, à l'exception du cas de direct marketing[348], la personne concernée exerçant son droit d'opposition devra faire valoir des raisons tenant à sa situation particulière[349].

---

344 Art. 17, § 1er, c), du RGPD.

345 Voy. *infra*, chapitre 1, section 7, « Droit d'opposition (art. 21 du RGPD) ».

346 Voy. *supra*, pts 75 à 77.

347 C. Bartolini et L. Siry, « The right to be forgotten in the light of the consent of the data subject », *op. cit.*, p. 226.

348 Voy. *infra*, pt 175.

349 C. Bartolini et L. Siry, « The right to be forgotten in the light of the consent of the data subject », *op. cit.*, p. 226. Pour plus d'informations sur la justification par la personne concernée de l'exercice de son droit d'opposition, voy. *infra*, pts 171 à 176.

v. Droit à l'effacement des données collectées dans le cadre de l'offre directe de services de la société de l'information aux enfants

80. Le droit à l'effacement au sens large englobe, enfin, le droit pour la personne concernée de demander l'effacement des données à caractère personnel collectées dans le cadre de l'offre directe de services de la société de l'information aux enfants[350]. Pour saisir la portée de ce droit, il convient de définir les termes « enfants » et « service de la société de l'information ».

Premièrement, sont considérées comme des « enfants », au sens du RGPD, les personnes de moins de 16 ans[351]. Précisons que les États membres peuvent prévoir par la loi un âge inférieur, pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans[352].

Deuxièmement, est considéré comme un « service de la société de l'information », un service au sens de l'article 1er, paragraphe 1er, b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil[353], c'est-à-dire tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services[354].

Un service presté « à distance » est un service fourni sans que les parties soient simultanément présentes[355].

Pour leur part, les termes « par voie électronique » font référence à un service envoyé à l'origine et reçu à destination au moyen d'équipements électroniques de traitement et de stockage de données, et qui est entièrement transmis, acheminé et reçu par fils, par radio, par moyens optiques ou par d'autres moyens électromagnétiques[356].

Enfin, un service presté « à la demande individuelle d'un destinataire de services » est un service fourni par transmission de données sur demande individuelle[357].

81. Lorsque des données à caractère personnel ont été collectées dans le cadre de l'offre directe de tels services de la société de l'information à

---

350 Art. 17, § 1er, f), du RGPD.

351 Art. 8, § 1er, al. 1er, du RGPD.

352 Art. 8, § 1er, al. 2, du RGPD.

353 Art. 4, 25), du RGPD.

354 Art. 1er, § 1er, b), de la directive 2015/1535/UE du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information, *J.O.U.E.*, 17 septembre 2015, L 241.

355 *Ibid.*

356 *Ibid.*

357 *Ibid.*

un enfant, la personne concernée pourra, à tout moment, demander que les données en cause soient effacées.

À l'instar de l'hypothèse d'un retrait de consentement, et à la différence de l'hypothèse de l'exercice du droit d'opposition[358], aucune justification ne devra être fournie par la personne concernée pour demander l'effacement de ces données.

Dans la même veine que le principe de transparence renforcée évoqué précédemment[359], ceci témoigne d'une volonté claire du RGPD d'octroyer une protection exacerbée aux enfants, compte tenu de leur plus grande vulnérabilité. Le considérant n° 38 exprime d'ailleurs clairement cet objectif :

> « Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel. Cette protection spécifique devrait, notamment, s'appliquer […] à la collecte de données à caractère personnel relatives aux enfants lors de l'utilisation de services proposés directement à un enfant ».

Le considérant n° 65 du RGPD précise d'ailleurs, à cet égard, que le droit à l'effacement au sens large est particulièrement pertinent :

> « Lorsque la personne concernée a donné son consentement à l'époque où elle était enfant et n'était pas pleinement consciente des risques inhérents au traitement, et qu'elle souhaite par la suite supprimer ces données à caractère personnel, en particulier sur l'internet. La personne concernée devrait pouvoir exercer ce droit nonobstant le fait qu'elle n'est plus un enfant ».

vi. Le cas particulier des données rendues publiques (art. 17, § 2, du RGPD)

82. La portée du droit à l'effacement au sens large, tel que consacré par l'article 17 du RGPD est, de surcroit, renforcée par le fait que le second paragraphe de cet article dispose que :

> « Lorsqu'il a rendu publiques les données à caractère personnel et qu'il est tenu de les effacer en vertu du paragraphe 1, le responsable du traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables, y compris d'ordre technique,

[358] Voy. *supra*, pt 79.
[359] Voy. *supra*, pt 14.

pour informer les responsables du traitement qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement par ces responsables du traitement de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci »[360].

Le principe même de cette obligation imposée au responsable de traitement initial de faire suivre cette demande d'effacement aux responsables de traitements ayant traité les données en cause en aval n'est pas nouveau, puisqu'il était déjà consacré à l'article 12, c), de la Directive[361].

Notons toutefois que, à la différence de l'article 12, c), de la Directive qui ne prévoyait un tel « droit de suite »[362] que dans l'hypothèse du droit à l'effacement *sensu stricto*, l'article 17, paragraphe 2, s'applique pour sa part non seulement au droit à l'effacement *sensu stricto*, mais également aux autres facettes du droit à l'effacement au sens large exposées ci-dessus[363].

83. Force est d'admettre qu'en pratique, il pourra s'avérer extrêmement compliqué pour le responsable de traitement ayant rendu accessibles sur internet les données en cause, d'identifier avec précision ces autres responsables de traitements ayant traité les données en aval, et de les informer de la demande d'effacement de la personne concernée, ce qui justifie que l'obligation imposée en vertu de l'article 17, paragraphe 2, du RGPD soit comprise comme étant une obligation de moyens, et non de résultat[364].

Notons toutefois que, selon C. Bartolini et L. Siry, il est parfaitement possible pour les responsables de traitements d'implémenter des solutions techniques permettant de tracer ces transmissions de données personnelles, afin de relayer cette demande d'effacement[365]. Ces auteurs justifient leur position en faisant valoir que, en règle générale, deux modèles techniques de partage de données sont utilisés, à savoir soit un modèle distribué, soit un modèle centralisé[366]. Dans le modèle distribué, le responsable

---

[360] Art. 17, § 2, du RGPD.

[361] 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 », *op. cit.*, p. 270.

[362] C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », note sous C.J.U.E., 22 décembre 2010, *R.D.T.I.*, n° 43, 2011, p. 78.

[363] 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 », *op. cit.*, p. 270.

[364] *Ibid.*, pp. 270-271.

[365] C. BARTOLINI et L. SIRY, « The right to be forgotten in the light of the consent of the data subject », *op. cit.*, p. 231.

[366] *Ibid.*

de traitement originaire garde une trace des tiers ayant accédé à et copié ces données, ce qui lui permet aisément d'identifier les tiers auxquels il doit relayer la demande d'effacement de la personne concernée[367]. Dans le modèle centralisé, les données en cause n'existent qu'auprès du responsable de traitement originaire, et toute dissémination apparente de ces données n'est, en réalité, que le résultat de l'établissement d'une référence vers ces données originaires, de sorte qu'il suffit au responsable de traitement de supprimer ces données originaires pour que l'effacement soit propagé sur ces sites tiers[368].

À vrai dire, il convient d'être plus nuancé, car présenter ces deux modèles de façon aussi absolue sur le plan technique revient à ignorer la réalité d'internet. De fait, dans le modèle distribué, il ne sera pas toujours possible d'identifier les tiers, puisque ceux-ci pourraient avoir fait usage de mécanismes techniques pour masquer leur identité, via un VPN[369] par exemple. De même, dans le modèle centralisé, il serait naïf de croire que les tiers accédant aux données originaires ne seront jamais en mesure de créer des copies des données, de sorte que, même après l'effacement par le responsable de traitement des données originaire, des copies de ces données subsisteront sur certains sites tiers. Dans un cas comme dans l'autre, il ne sera donc pas si évident de donner corps à l'exigence de cet article 17, paragraphe 2, du RGPD.

En revanche, on pourrait envisager que le responsable de traitement fasse usage du registre des activités de traitements que celui-ci est contraint de tenir en vertu de l'article 30 du RGPD[370], pour identifier les responsables de traitements auprès de qui il doit relayer ladite demande d'effacement. De fait, ce registre doit notamment comporter des informations relatives aux « catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales »[371]. Notons toutefois qu'il est ici fait référence aux « catégories de destinataires », ce qui laisse à penser que ce registre ne contiendra pas la liste précise de l'ensemble des destinataires auprès desquels il devrait relayer la demande d'effacement[372].

---

367 *Ibid.*

368 *Ibid.*

369 « *Virtual Private Network* ». En français, un « réseau privé virtuel ».

370 Voy. à ce sujet la contribution de Franck Dumortier intitulée « La sécurité des traitement de données, les analyses d'impact et les violations de données », dans le présent ouvrage.

371 Art. 30, § 1er, d), du RGPD.

372 Voy. *infra*, pt 85.

84. Enfin, il convient de se demander si cet article 17, paragraphe 2, du RGPD n'est pas redondant avec l'article 19 du RGPD, qui est la version modernisée de l'article 12, c), de la Directive, et qui dispose que :

> « Le responsable du traitement **notifie à chaque destinataire auquel les données à caractère personnel ont été communiquées** toute rectification ou *tout effacement* de données à caractère personnel ou toute limitation du traitement effectué conformément à l'article 16, à l'article 17, paragraphe 1, et à l'article 18, **à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés. Le responsable du traitement fournit à la personne concernée des informations sur ces destinataires si celle-ci en fait la demande** » (nous soulignons).

Le champ d'application de cet article 19 du RGPD est certes plus large que celui de l'article 17, paragraphe 2, du RGPD, puisqu'il vise non seulement le droit à l'effacement au sens large, mais également le droit de rectification, exposé *supra*[373], et le droit à la limitation du traitement que nous analyserons *infra*[374]. Cela étant, il convient de se demander si, dès lors que l'article 19 du RGPD s'applique au droit à l'effacement au sens large, l'article 17, paragraphe 2, du RGPD n'est pas redondant.

85. En réalité, il ressort de la comparaison de ces deux dispositions que celles-ci ne sont pas formulées de façon totalement identique.

Tout d'abord, les récipiendaires de la notification envisagée ne sont pas les mêmes dans ces deux dispositions. Ainsi, dans le cas de l'article 17, paragraphe 2, du RGPD, les récipiendaires sont les responsables de traitements qui traitent les données en aval. En revanche, la notification de l'article 19 du RGPD sera adressée à un plus grand nombre de récipiendaires, puisqu'elle doit être notifiée « à chaque destinataire[375] auquel les données à caractère personnel ont été communiquées ». Sont donc également visés les sous-traitants.

Ensuite, « l'effort » devant être fourni par le responsable de traitement n'est pas défini de la même manière dans ces deux dispositions. L'article 19 du RGPD prévoit en effet que le responsable de traitement doit procéder à la notification « à moins [que celle-ci] se révèle impossible ou exige des efforts disproportionnés ». L'article 17, paragraphe 2, du RGPD est, pour sa part, un peu plus précis, puisqu'il dispose que « le responsable

---

373 Voy. Chapitre 1, section 3, « Droit de rectification (art. 16 du RGPD) ».

374 Voy. Chapitre 1, section 5, « Droit à la limitation du traitement (art. 18 du RGPD) ».

375 Au sens du RGPD, le destinataire est : « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers » (art. 4, 9), du RGPD).

de traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables, y compris d'ordre technique » pour s'acquitter de son obligation.

Enfin, l'article 19 du RGPD octroie à la personne concernée, à la condition qu'elle en fasse la demande, le droit de recevoir des informations relatives aux destinataires de la notification en cause[376], tandis que l'article 17, paragraphe 2, du RGPD reste silencieux à cet égard.

Notons sur ce dernier point, qu'en vertu de l'article 13 du RGPD, la personne concernée a déjà dû, en principe, recevoir des informations concernant les destinataires ou les catégories de destinataires à qui le responsable du traitement a communiqué les données à caractère personnel[377]. Cela étant, il parait réaliste de considérer que, dans le cadre de cette obligation d'information préalable, le responsable de traitement se contentera bien souvent de faire référence à des catégories générales de destinataires, en indiquant, par exemple, que les données sont communiquées à ses « partenaires commerciaux ». En revanche, la personne concernée devrait être en mesure d'obtenir une information plus précise par le biais de cet article 19 du RGPD, puisqu'il est exigé du responsable de traitement qu'il fournisse, à la personne concernée en faisant la demande, la liste précise de « chaque destinataire » à qui il a communiqué, par le passé, les données en cause.

En conclusion, l'article 19 du RGPD est donc plus détaillé et a des conséquences plus vastes que l'article 17, paragraphe 2, du RGPD, hormis sur la question de l'effort devant être fourni par le responsable de traitement. Il eût donc sans doute mieux valu se limiter à l'inclusion du seul article 19 du RGPD, tout en remplaçant la description actuelle de l'effort devant être fourni par le responsable de traitement qui y est contenue, par celle contenue à l'article 17, paragraphe 2, du RGPD. Il est d'ailleurs étonnant que cette redondance entre les deux articles en cause n'ait jamais été soulignée lors des discussions menant à l'adoption du RGPD, car elle était déjà présente dans le texte de la proposition initiale de la Commission[378]. En tout état de cause, tout responsable de traitement confronté à une demande d'effacement devra, au vu de la formulation actuelle du RGPD, être attentif non seulement aux exigences découlant de l'article 17, paragraphe 2, du RGPD, mais aussi à celles, plus détaillées, contenues à l'article 19 du RGPD.

---

376 Art. 19 du RGPD.

377 Art. 13, § 1er, e), du RGPD.

378 Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), 25 janvier 2012, COM(2012) 11 final, art. 13 (« Droits à l'égard des destinataires ») et 17, § 2 (« Droit à l'oubli numérique et à l'effacement »).

2° Les exceptions au droit à l'effacement au sens large (art. 17, § 3, du RGPD)

86. Le droit à l'effacement au sens large, n'est toutefois pas absolu, et il ne sera pas applicable dans la mesure où le traitement des données est nécessaire :

> « a) à l'exercice du droit à la liberté d'expression et d'information ;
> b) pour respecter une obligation légale qui requiert le traitement prévu par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
> c) pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9, § 2, h) et i), ainsi qu'à l'article 9, § 3 ;
> d) à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, § 1, dans la mesure où le droit visé au § 1 est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement ; ou
> e) à la constatation, à l'exercice ou à la défense de droits en justice »[379].

En pareil cas, la conservation ultérieure des données par le responsable de traitement sera considérée comme licite et la personne concernée ne pourra s'y opposer[380].

Certaines de ces exceptions appellent à des précisions supplémentaires.

87. Concernant, tout d'abord, la question du conflit entre le droit à l'effacement au sens large et le droit à la liberté d'expression et d'information, le considérant n° 153 du RGPD rappelle, à l'instar de la jurisprudence européenne en la matière[381], que les notions liées à la liberté d'expression, et notamment la notion de journalisme, doivent être interprétées largement[382], et ce, « pour tenir compte de l'importance du droit à la liberté d'expression dans toute société démocratique »[383].

---

[379] Art. 17, § 3, du RGPD.

[380] Considérant n° 65 du RGPD ; S. CARNEROLI, *Le droit à l'oubli : du devoir de mémoire au droit à l'oubli*, Bruxelles, Larcier, 2016, p. 73.

[381] Voy. not. Cour eur. D.H., arrêt *Times Newspapers Limited (nos 1 et 2) c. Royaume-Uni*, 10 mars 2009, req. nos 3002/03 et 23676/03 et C.J.U.E., 16 décembre 2008, *Satakunnan Markkinapörssi et Satamedia*, affaire C-73/07, cités par S. CARNEROLI, *Le droit à l'oubli : du devoir de mémoire au droit à l'oubli*, *op. cit.*, p. 74.

[382] S. CARNEROLI, *Le droit à l'oubli : du devoir de mémoire au droit à l'oubli*, *op. cit.*, p. 74.

[383] Considérant n° 153 du RGPD.

Par ailleurs, il convient de souligner que le droit à la liberté d'expression et d'information englobe « l'activité d'archivage des articles de la presse audiovisuelle ou écrite »[384]. De fait, le considérant n° 153 du RGPD précise que :

> « Il y a lieu de prévoir des dérogations ou des exemptions à certaines dispositions du présent règlement si cela est nécessaire pour concilier le droit à la protection des données à caractère personnel et le droit à la liberté d'expression et d'information [...] Tel devrait notamment être le cas des traitements de données à caractère personnel dans le domaine de l'audiovisuel et dans les documents d'archives d'actualités et bibliothèques de la presse ».

Comme le souligne S. Carneroli :

> « L'archivage de la presse électronique est donc expressément considéré par le législateur européen comme une activité qui justifie en tant que telle qu'il soit dérogé aux droits que peuvent faire valoir les personnes concernées sur les données personnelles qui sont traitées par les médias »[385].

Enfin, il découle de la jurisprudence de la Cour européenne des droits de l'homme que tant l'écoulement du temps que « l'intérêt historique et l'intérêt public, la nature des faits et la personne en cause [devront] être pris en considération pour résoudre [ce] conflit »[386].

88. Concernant les motifs d'intérêt public dans le domaine de la santé publique permettant de déroger à l'application du droit à l'effacement au sens large, il convient de se référer à l'article 9 du RGPD. Ainsi, en vertu de l'article 9, paragraphe 2, du RGPD, seront considérés comme rencontrant un tel objectif d'intérêt public dans le domaine de la santé publique :

> « h) [les traitements nécessaires] aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé soumis [à une obligation de secret professionnel] ; [et]

---

384 S. Carneroli, *Le droit à l'oubli : du devoir de mémoire au droit à l'oubli, op. cit.*, p. 74.

385 S. Carneroli, *Le droit à l'oubli : du devoir de mémoire au droit à l'oubli, op. cit.*, p. 75.

386 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 », *op. cit.*, pp. 258-259.

> i) [les traitements nécessaires] pour des motifs […] tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel »[387].

Les personnes concernées ne pourront donc demander l'effacement de données traitées pour l'un des motifs susmentionnés, ce qui fait sens, dès lors qu'il est légitime que ces motifs d'intérêt public prévalent sur les intérêts particuliers des personnes concernées.

89. Pour ce qui est de l'exception à des fins archivistiques dans l'intérêt public, il convient de pointer que le considérant n° 158 du RGPD définit ce qu'il convient d'entendre par « services d'archives »[388]. Sont ainsi visés :

> « Les autorités publiques ou les organismes publics ou privés qui conservent des archives dans l'intérêt public devraient être des services qui, en vertu du droit de l'Union ou du droit d'un État membre, ont l'obligation légale de collecter, de conserver, d'évaluer, d'organiser, de décrire, de communiquer, de mettre en valeur, de diffuser des archives qui sont à conserver à titre définitif dans l'intérêt public général et d'y donner accès »[389].

Notons qu'il est précisé dans ce considérant n° 158 que le RGPD ne s'applique pas aux personnes décédées[390].

À titre d'exemple, cette exception à des fins archivistiques devrait faire obstacle à l'effacement de données personnelles traitées en vue de « fournir des informations précises relatives au comportement politique sous les régimes des anciens États totalitaires, aux génocides, aux crimes contre l'humanité, notamment l'Holocauste, ou aux crimes de guerre »[391].

90. Ce même considérant n° 158 du RGPD fournit également quelques explications sur l'exception à des fins de recherche scientifique. Il indique ainsi que la notion de « fins de recherche scientifique » devrait être interprétée largement, et précise que sont notamment visés le développement

---

387 Art. 9, § 2, h) et i), du RGPD.
388 S. Carneroli, *Le droit à l'oubli : du devoir de mémoire au droit à l'oubli*, *op. cit.*, p. 75.
389 Considérant n° 158 du RGPD.
390 S. Carneroli, *Le droit à l'oubli : du devoir de mémoire au droit à l'oubli*, *op. cit.*, p. 75.
391 Considérant n° 158 du RGPD.

et la démonstration de technologies, la recherche fondamentale, la recherche appliquée, la recherche financée par le secteur privé et les études menées dans l'intérêt public dans le domaine de la santé publique[392].

Cette exception à l'application du droit à l'effacement au sens large se justifie par la volonté de laisser aux chercheurs la possibilité d'acquérir de nouvelles connaissances en combinant des informations issues de registres, notamment dans le domaine médical, en vue de lutter contre les maladies cardiovasculaires, le cancer et la dépression[393]. Dans le domaine des sciences sociales, cette exception devrait, par exemple, permettre de favoriser les recherches centrées autour d'un certain nombre de conditions sociales telles que le chômage et l'éducation[394].

Précisons, enfin, qu'en cas de traitements à des fins scientifiques, le responsable de traitement devra également respecter d'autres dispositions législatives pertinentes, telles que celles relatives aux essais cliniques[395].

91. Enfin, le considérant n° 162 du RGPD nous éclaire sur ce qu'il convient d'entendre par la notion de « fins statistiques », à savoir « toute opération de collecte et de traitement de données à caractère personnel nécessaires pour des enquêtes statistiques ou la production de résultats statistiques »[396].

3° Modalités d'exercice du droit à l'effacement au sens large

92. Au sujet des modalités d'exercice du droit à l'effacement au sens large, l'article 17, paragraphe 1er, du RGPD dispose simplement que l'effacement des données doit être fait « dans les meilleurs délais », sans toutefois préciser ce qu'il convient d'entendre par là.

Ce délai sera vraisemblablement fonction de la nature, de l'ampleur et du contexte de la demande, ainsi que des moyens techniques dont dispose le responsable de traitement[397].

93. Par ailleurs, l'article 12 du RGPD, qui régit de façon commune les modalités d'exercice de l'ensemble des droits de la personne concernée[398],

[392] *Ibid.*
[393] Considérant n° 157 du RGPD.
[394] *Ibid.*
[395] Considérant n° 158 du RGPD.
[396] Considérant n° 162 du RGPD.
[397] C. Vande Vorst, « Algemene verordening gegevensbescherming : vijf nieuwigheden van dichterbij bekeken », *op. cit.*, p. 82.
[398] Voy. art. 12, §§ 2 à 6 du RGPD.

et que nous analyserons plus en détail *infra*[399], dispose qu'une demande de la personne concernée relative à l'exercice de l'un de ses droits, en ce compris le droit à l'effacement au sens large, doit être traitée « **dans les meilleurs délais** et en tout état de cause dans un délai d'un mois à compter de la réception de la demande »[400], sauf exception[401].

Il nous semble donc que les termes « dans les meilleurs délais » de l'article 17, paragraphe 1er, du RGPD doivent être interprétés à l'aune de cet article 12, paragraphe 3, du RGPD qui contient les mêmes termes.

Or, nous verrons *infra*[402], qu'en vertu de l'article 12 du RGPD, le responsable de traitement doit, en tout état de cause, fournir des informations à la personne concernée dans un délai d'un mois à compter de la réception de la demande, que ce soit pour l'informer :

- Des mesures prises à la suite de sa demande[403] ; ou
- Du fait qu'il estime que le délai pour traiter la demande doit être prolongé de deux mois et les motifs justifiant cette prolongation[404] ; ou
- Des motifs de son inaction et de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle et de former un recours juridictionnel[405].

D'après nous, il serait cohérent qu'il en soit de même pour l'article 17, paragraphe 1er, du RGPD.

94. De surcroit, il conviendra de faire une distinction entre le délai de réaction d'un mois, tel qu'identifié ci-dessus, et le délai d'effacement effectif, dès lors que, s'il est tout à fait envisageable d'exiger du responsable de traitement qu'il réagisse dans un délai rapide en communiquant sa décision à la personne concernée, l'effacement concret des données pourrait, pour sa part, nécessiter un délai plus long, au vu des implications techniques et opérationnelles liées à cet effacement[406].

Ceci pourrait notamment être le cas si le responsable de traitement a un système informatique mal géré en amont, la demande nécessitant alors une certaine dose d'investigations pour retrouver où sont stockées

---

399 Voy. chapitre 1, section 9, relative aux « Modalités de l'exercice des droits de la personne concernée (art. 12, §§ 2 à 6) ».

400 Art. 12, § 3, du RGPD.

401 Pour plus de précisions sur cette question, voy. *infra*, pts 190 et 191.

402 Voy. pts 190 et 191.

403 Art. 12, § 3, du RGPD.

404 *Ibid.*

405 Art. 12, § 4, du RGPD.

406 C. Vande Vorst, « Algemene verordening gegevensbescherming : vijf nieuwigheden van dichterbij bekeken », *op. cit.*, p. 82.

les données en cause. Il n'en reste pas moins que ceci ne devrait pas servir d'excuse pour retarder inutilement l'effacement concret, dès lors que, en présence d'un système bien construit, le délai d'un mois pour procéder à l'effacement est parfaitement tenable.

95. Enfin, précisons qu'aucun paiement ne peut être exigé pour prendre toute mesure au titre du droit à l'effacement au sens large, à moins que la demande de la personne concernée ne s'avère manifestement infondée ou excessive[407].

§ 3. Le « droit à l'oubli » : un concept plus vaste que le droit à l'effacement au sens large, tel que consacré par l'article 17 du RGPD

a) Portée du « droit à l'oubli »

96. Le « droit à l'oubli » présente, selon nous, une portée plus étendue que le droit à l'effacement au sens large, qui pourrait, ce faisant, être qualifié de « droit à l'oubli incomplet ». Ainsi, selon l'analyse qui en est faite par la professeure C. de Terwangne, à laquelle nous nous rallions, le « droit à l'oubli » couvre :

> « - le droit au repentir et à changer d'avis à l'égard de ce que l'on a diffusé auparavant ou accepté que l'on fasse avec ses données ;
> - le droit de ne pas voir en permanence rappelé son passé, de ne pas voir son passé encombrer le présent et hypothéquer l'avenir ;
> - le droit d'obtenir qu'une personne ne conserve plus ce qu'elle savait parce que ce n'est plus légitime, le principe de finalité ne le justifiant plus ou parce que c'est non conforme aux règles de protection des données ;
> - le droit de refuser la décontextualisation des données en luttant principalement contre la puissance des moteurs de recherche sur Internet, tout en admettant éventuellement que les données demeurent dans leur contexte initial »[408].

97. À y regarder de plus près, il s'agit d'un droit englobant non seulement le droit à l'effacement au sens large – composé du droit à l'effacement *sensu stricto*, du droit à l'effacement comme conséquence automatique du

---

[407] Art. 12, § 5, du RGPD. Pour plus de précisions sur cette question, voy. *infra*, pt 188.

[408] 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 », *op. cit.*, pp. 273-274.

principe de finalité, du droit à l'effacement suite au retrait de consentement et du droit à l'effacement suite à l'exercice du droit d'opposition[409]–, mais également le droit au déréférencement des résultats de moteurs de recherche, consacré par la Cour de justice de l'Union européenne dans son arrêt *Google Spain*[410], et à l'analyse duquel nous nous contentons de renvoyer ici[411]. Rappelons simplement la différence fondamentale entre ce droit au déréférencement et le droit à l'effacement au sens large. Ainsi, si ces deux droits relèvent du concept plus large du « droit à l'oubli », ils divergent néanmoins par leur « degré d'effacement des données »[412]. De fait, en vertu du droit à l'effacement au sens large, le responsable de traitement doit, en principe[413], effacer toutes les données en cause de la personne concernée, tandis que, en vertu du droit au déréférencement, seule l'indexation, dans les moteurs de recherches, du lien vers ces données (données « secondaires ») doit être effacée, et non les données en tant que telles qui se trouvent sur le site source[414] (« données originaires »). Bien entendu, ce droit au déréférencement conduit tout de même à l'effacement de certaines données, puisque le responsable de traitement auprès de qui la demande de déréférencement est introduite par la personne concernée devra effacer certaines données de sa base de données, à savoir les résultats associés à une recherche menée sur la base du nom de cette personne concernée.

98. Cette conception large du « droit à l'oubli » démontre bien que la volonté de mettre en place un tel « droit à l'oubli » était ancrée dans la finalité de renforcement de l'autodétermination informationnelle de la personne concernée, visant à rendre à la personne concernée le contrôle sur les données à caractère personnel la concernant[415].

Ces réflexions autour de la restitution à la personne concernée du contrôle sur ses données sont particulièrement pertinentes au regard des spécificités de l'internet[416]. De fait, cet outil numérique implique

---

[409] *Ibid.*, p. 274. Sur la portée de ce droit à l'effacement au sens large, voy. *supra*, chapitre 1, section 4, § 2.

[410] C.J.U.E. (gde ch.), 13 mai 2014, *Google Spain SL et Google Inc.*, C-131/12.

[411] Voy. *supra*, chapitre 1, section 4, § 1.

[412] C. Vande Vorst, « Algemene verordening gegevensbescherming : vijf nieuwigheden van dichterbij bekeken », *op. cit.*, p. 82.

[413] Voy. *supra*, pt 70.

[414] C. Vande Vorst, « Algemene verordening gegevensbescherming : vijf nieuwigheden van dichterbij bekeken », *op. cit.*, p. 83.

[415] 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 », *op. cit.*, p. 252.

[416] *Ibid.*, p. 248.

un « *eternity effect* »[417], à savoir que, à la différence du monde physique, l'effacement dans le monde numérique ne sera jamais automatique, et implique une action volontaire et réfléchie[418].

L'effacement dans le monde numérique est donc dépendant d'une action concrète, qui ne va pas nécessairement de soi, dès lors qu'il est plus couteux en temps, et donc financièrement, d'effacer ou d'anonymiser des données que de simplement les conserver[419].

Ceci peut notamment être illustré par le phénomène des réseaux sociaux, pour lesquels le « droit à l'oubli » s'avère particulièrement pertinent[420], dès lors qu'il n'est pas rare que des photos ou des messages qui ont été postés plusieurs années auparavant, lorsque la personne concernée était dans un autre état d'esprit ou était simplement moins prudente, refassent surface alors que cette personne croyait ces éléments « enterrés », ce qui pourrait lui causer un préjudice.

b) Effets de l'exercice du « droit à l'oubli »

99. L'exercice du « droit à l'oubli », dont la portée a été analysée ci-dessus, peut engendrer des conséquences variées, telles que l'effacement ou l'anonymisation des données en tant que telles, ou encore le déréférencement, dans les moteurs de recherches, du lien vers ces données[421].

En sus de ces effets « classiques », d'autres conséquences de l'exercice du « droit à l'oubli » pourraient être intégrées dans l'arsenal des solutions envisageables afin d'atteindre un équilibre entre les droits et intérêts des parties en présence, telles que « l'accès restreint aux données […] d'autres formes de publicité ou l'arrêt de certaines formes de diffusion […] [ou encore] l'adjonction d'une information supplémentaire aux données [par exemple, un avertissement ou le point de vue de la personne concernée] »[422].

---

[417] S. Walz, « Relationship between the freedom of the press and the right for informational privacy in the emerging Information society », *19e Conférence internationale des commissaires à la protection des données*, Bruxelles, 17-19 septembre 1997, p. 3.

[418] 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 », *op. cit.*, p. 248.

[419] *Ibid.*, p. 249.

[420] C. de Terwangne, « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », *op. cit.*, p. 103.

[421] 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 », *op. cit.*, pp. 268-269.

[422] *Ibid.*

SECTION 5. – Droit à la limitation du traitement (art. 18 du RGPD)

§ 1. Portée du droit

100. En vertu de l'article 18 du RGPD, la personne concernée a le droit d'obtenir du responsable de traitement la limitation du traitement dans quatre hypothèses, à savoir lorsque :

– l'exactitude des données à caractère personnel est contestée par la personne concernée, pendant une durée permettant au responsable du traitement de vérifier leur exactitude ou non [exercice du droit de rectification][423] ;
– le traitement est illicite et la personne concernée s'oppose à l'effacement des données et exige à la place la limitation de leur utilisation [réservation de preuves dans le cadre d'un litige opposant la personne concernée au responsable de traitement][424] ;
– le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement, mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice [réservation de preuves dans le cadre d'un litige opposant la personne concernée au responsable de traitement ou à un tiers][425] ;
– la personne concernée s'est opposée au traitement en vertu de l'article 21, paragraphe 1er, du RGPD, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée [exercice du droit d'opposition][426].

Tout comme le droit de rectification[427], ce droit à la limitation du traitement était déjà couvert par la Directive sous le vocable de « droit de verrouillage », dans un article 12 qui regroupait le droit d'accès, le droit de rectification, le droit à l'effacement et le droit de limitation de la personne concernée[428]. Cela fait sens dès lors que le droit d'accès peut, comme nous l'avons souligné ci-dessus[429], être à l'origine de l'exercice ultérieur de

[423] Art. 18, § 1er, a), du RGPD.
[424] Art. 18, § 1er, b), du RGPD.
[425] Art. 18, § 1er, c), du RGPD.
[426] Art. 18, § 1er, d), du RGPD.
[427] Voy. *supra*, pts 51 à 53.
[428] Art. 12 de la Directive.
[429] Voy. *supra*, pt 39.

ces autres droits de la personne concernée[430]. Rappelons que ce droit à la limitation du traitement peut également être déclenché suite à l'exercice du droit d'opposition[431].

Comme indiqué *supra*[432], les auteurs du RGPD ont cependant adopté une approche distincte de la Directive, en prévoyant un article spécifique pour chacun des droits de la personne concernée, et donc un article 18 dédié exclusivement au droit à la limitation du traitement.

101. En pratique, si la personne concernée exerce son droit à la limitation du traitement dans l'une des hypothèses visées à l'article 18, paragraphe 1er, du RGPD, le responsable de traitement devra s'abstenir d'accomplir quel qu'autre traitement que ce soit sur les données en cause, pour le temps nécessaire à l'exercice de ce droit à la limitation. En d'autres mots, les données à caractère personnel seront, pour reprendre les termes de la Directive, « verrouillées » pendant un certain laps de temps.

Ainsi, durant cette période, ces données à caractère personnel ne peuvent, à l'exception de la conservation, être traitées qu'avec le consentement de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice, pour la protection des droits d'une autre personne physique ou morale, ou encore pour des motifs importants d'intérêt public de l'Union ou d'un État membre[433].

Précisons également que la personne concernée devra être informée par le responsable de traitement avant que la limitation du traitement ne soit levée[434].

102. Parallèlement à ce que nous avions exposé concernant le droit de rectification[435], l'article 18 du RGPD ne permet pas d'avoir une vision complète de la portée exacte du droit à la limitation du traitement.

En effet, comme le prévoyait déjà la Directive[436], le « droit de suite »[437] contenu à l'article 19 du RGPD s'applique également au droit à la limitation du traitement. Ainsi, le responsable de traitement est tenu de noti-

---

[430] C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », note sous C.J.U.E., 22 décembre 2010, *R.D.T.I.*, n° 43, 2011, p. 77.

[431] Art. 18, § 1er, d), du RGPD.

[432] Voy. pt 51.

[433] Art. 18, § 2, du RGPD.

[434] Art. 18, § 3, du RGPD.

[435] Voy. *supra*, pts 52 à 53.

[436] Voy. art. 12, c) de la Directive.

[437] C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », *op. cit.*, p. 78.

fier, à chaque destinataire auquel les données à caractère personnel ont été communiquées, toute limitation du traitement effectuée conformément à l'article 16 du RGPD, à moins qu'une telle communication ne se révèle impossible ou exige des efforts disproportionnés dans le chef du responsable de traitement[438].

À nouveau, et à condition qu'elle en fasse la demande, la personne concernée a le droit de recevoir des informations relatives à ces destinataires[439].

103. Le droit à la limitation du traitement comporte donc, comme le droit de rectification, une double facette, à savoir, d'une part, le droit d'obtenir la limitation du traitement dans les quatre hypothèses visées à l'article 18, paragraphe 1er, du RGPD, et d'autre part, le bénéfice de l'obligation imposée au responsable de traitement de « faire suivre » cette limitation du traitement en la notifiant aux destinataires desdites données à caractère personnel, sauf si cela exige des efforts disproportionnés[440].

§ 2. Exercice du droit

104. Enfin, étant donné que les modalités de l'exercice de ce droit à la limitation du traitement ne sont pas contenues dans l'article 18 du RGPD relatif à ce droit, mais dans l'article 12 du RGPD, qui régit de façon commune les modalités d'exercice de l'ensemble des droits de la personne concernée[441], nous invitons le lecteur à se référer à l'analyse de ces modalités que nous avons effectuée *infra*[442].

Précisons simplement, à ce stade, que cet article 12 dispose qu'une demande de la personne concernée relative à l'exercice de ce droit doit être traitée « dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande »[443], sauf exception[444]. Qui plus est, aucun paiement ne peut être exigé pour prendre toute mesure au titre du droit à la limitation du traitement, à moins que la demande de la personne concernée ne s'avère manifestement infondée ou excessive[445].

---

438 Art. 19 du RGPD ; art. 12, c), de la Directive.

439 Art. 19 du RGPD.

440 Sur cette question de la difficulté pratique potentielle de définir ce qui doit être considéré comme étant un effort proportionné ou non, voy. *supra*, pt 53.

441 Voy. art. 12, §§ 2 à 6, du RGPD.

442 Voy. chapitre 1, section 9, relative aux « Modalités de l'exercice des droits de la personne concernée (art. 12, §§ 2 à 6) ».

443 Art. 12, § 3, du RGPD.

444 Pour plus de précisions sur cette question, voy. *infra*, pts 190 et 191.

445 Art. 12, § 5, du RGPD. Pour plus de précisions sur cette question, voy. *infra*, pt 188.

SECTION 6. – Droit à la portabilité des données (art. 20 du RGPD)

105. Comme annoncé en guise d'introduction à la présente contribution, l'instauration d'un droit à la portabilité des données est une des nouveautés phares du RGPD, qui risque de susciter un nombre important de débats autour de la portée exacte de cette disposition, et de l'impact qu'elle pourra avoir sur les responsables de traitements et leurs sous-traitants, ainsi que sur les personnes concernées.

L'incertitude planant autour de ce nouveau droit résulte notamment du fait que le texte de l'article 20 du RGPD est, somme toute, assez laconique, alors même qu'il semble évident pour tout un chacun que les conséquences de l'intégration de ce droit dans le RGPD seront loin d'être marginales.

106. Conscient de l'existence d'un réel besoin, dans le chef des acteurs de terrain, de disposer de précisions au sujet de cette création nouvelle, le Groupe 29 a, de façon bienvenue, adopté, en date du 13 décembre 2016, des lignes directrices sur ce droit à la portabilité des données à caractère personnel[446]. Ces lignes directrices ont ensuite été révisées le 5 avril 2017[447], suite à une période de consultation publique. Nous ferons, dans la suite de notre propos, référence à cette version révisée, sauf lorsque nous discuterons de certains éléments contenus uniquement dans la première version et n'ayant pas été repris dans la version révisée.

L'intention du Groupe 29 est de permettre aux responsables de traitements et à leurs sous-traitants de se préparer au mieux à l'entrée en vigueur de cette disposition, et de clarifier ce concept de portabilité des données à caractère personnel, afin de permettre aux personnes concernées d'invoquer efficacement ce droit[448].

Les lignes qui suivent ont donc pour vocation d'analyser, à l'aune de ces lignes directrices du Groupe 29, les enjeux concrets de ce nouveau droit à la portabilité des données.

§ 1. Objectifs sous-jacents

107. Les objectifs ayant justifié l'adoption de cette disposition ne sont pas apparents dans le texte de l'article 20 du RGPD, mais un embryon d'explication peut être trouvé dans le considérant n° 68 du RGPD, qui

[446] Groupe 29, Guidelines on the right to « data portability », WP 242, 13 December 2016.
[447] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017.
[448] *Ibid.*, p. 4.

nous indique que ce droit vise à renforcer le contrôle que les personnes concernées exercent sur leurs propres données.

Se trouve ainsi traduite la volonté de renforcer le « *data subject empowerment* », à savoir le pouvoir de contrôle[449] qu'a la personne concernée sur ses données à caractère personnel, puisque ce droit lui permettra de « déplacer, copier ou transmettre facilement des données personnelles d'un environnement IT à un autre »[450].

En réalité, cet objectif de « *data subject empowerment* » est traduit en deux sous-objectifs.

108. D'une part, dans une conception stricte de la notion de « *data subject empowerment* », ce droit à la portabilité des données « représente une opportunité de "rééquilibrer" la relation entre les personnes concernées et les responsables de traitements »[451], et ce, « au travers de l'affirmation des droits personnels et du contrôle des individus sur les données à caractère personnel les concernant »[452].

Cet objectif est d'ailleurs transversal dans le RGPD, et dépasse le cadre du droit à la portabilité des données[453].

Notons, par ailleurs, que le « *data subject empowerment* » irradie également la Convention 108 modernisée[454] dans le préambule duquel l'accent est mis sur la dignité humaine, sur l'autonomie personnelle et l'autodétermination informationnelle liée au contrôle exercé par la personne concernée sur les données à caractère personnel la concernant[455].

---

[449] Ce qui est consacré ici est bien un droit de « contrôle » de la personne concernée sur ses données, et non un quelconque droit de « propriété ». Il convient en effet de ne pas confondre ces deux concepts, leur portée potentielle étant totalement différente.

[450] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 4. Traduction libre de : « *move, copy or transmit personal data easily from one IT environment to another* ».

[451] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 4. Traduction libre de : « *by affirming individuals' personal rights and control over the personal data concerning them* ».

[452] *Ibid.* Traduction libre de : « *represents an opportunity to "re-balance" the relationship between data subject and data controllers* ».

[453] Voy. not. *supra*, chapitre 1, section 1, relative au « Droit d'être informée de l'existence de traitements la concernant », qui a pour finalité de réduire le déséquilibre informationnel entre le responsable de traitement et la personne concernée, afin de permettre à cette dernière d'être parfaitement au fait de l'ensemble des traitements portant sur ses données personnelles, et des droits qu'elle est en mesure de faire valoir.

[454] Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), adoptée à Elseneur (Danemark) les 17 et 18 mai 2018, CM/Inf(2018)15-final.

[455] C. DE TERWANGNE, « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », *op. cit.*, pp. 91-92.

109. D'autre part, et dans une conception plus large de la notion de « *data subject empowerment* », ce droit à la portabilité doit permettre à la personne concernée de pouvoir plus facilement changer de fournisseur de service[456].

Dans sa première version de décembre 2016, le Groupe 29 avait même indiqué qu'il s'agissait là de « l'objectif principal »[457] de ce nouveau droit, car il devrait faciliter la création de nouveaux services, ce qui s'inscrit parfaitement dans la stratégie du législateur européen de création d'un marché digital unique[458].

Cette indication a cependant été supprimée dans la version révisée d'avril 2017, le Groupe 29 indiquant à présent que le RGPD vise à réguler les traitements de données à caractère personnel, et non à traiter de questions de droit de la concurrence[459]. La version révisée précise d'ailleurs dorénavant que l'objectif principal de ce droit est de promouvoir le « *data subject empowerment* »[460].

Il n'empêche que la création de ce nouveau droit à la portabilité laisse transparaitre l'impact non-négligeable qu'a eu l'apparition des réseaux sociaux sur les réflexions de modernisation de la Directive, ayant abouti à l'adoption du RGPD[461]. Cela témoigne également de la volonté claire d'éviter que les personnes concernées ne soient « coincées »[462] 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, 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.).

§ 2. Portée du droit

110. Dans certaines hypothèses bien définies[463], l'article 20 du RGPD confère à la personne concernée le droit de recevoir les données à carac-

---

[456] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 4.

[457] « *The primary aim* ».

[458] Groupe 29, Guidelines on the right to « data portability », WP 242, 13 December 2016, p. 4.

[459] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 4.

[460] *Ibid.*, p. 4, note infrapaginale n° 1.

[461] D. DE BOT, « De uitvoering van de algemene verordening gegevensbescherming – enkele bemerkingen bij de Belgische context », *T.V.W.*, 2016/3, p. 221.

[462] « *Lock-in* ».

[463] Voy. *infra*, chapitre 1, section 6, § 2, a).

tère personnel la concernant qu'elle a fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, ainsi que le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle[464].

À l'instar de la démarche opérée par le Groupe 29, il convient de mettre en lumière le champ d'application de ce nouveau droit (a), ses principaux éléments constitutifs (b) et les modalités d'exercice de ce droit (c)[465]. Enfin, nous exposerons en quoi ce droit à la portabilité se distingue du droit d'accès (d).

a) Champ d'application du droit à la portabilité

111. Le champ d'application du droit à la portabilité est limité, d'une part, à certaines catégories de traitements, et d'autre part, à certaines catégories de données.

1° Catégories de traitements auxquels ce droit s'applique

112. En vertu de l'article 20 du RGPD, la personne concernée pourra invoquer son droit à la portabilité des données lorsque le traitement :

- Est effectué à l'aide de procédés automatisés[466] ; *et*
- Est fondé :
  - Sur le consentement de la personne concernée en application de l'article 6, paragraphe 1er, a), ou de l'article 9, paragraphe 2, a), du RGPD[467] ; *ou*
  - Sur un contrat[468] en application de l'article 6, paragraphe 1er, b), du RGPD[469].

113. Il n'existe donc pas de « *droit général à la portabilité des données* »[470], dès lors que l'article 20 du RGPD précise que ce droit ne s'applique pas

[464] Art. 20, § 1er, du RGPD.

[465] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, pp. 4-20.

[466] Art. 20, § 1er, b), du RGPD.

[467] Art. 20, § 1er, a), du RGPD.

[468] Le Groupe 29 indique ainsi, à titre d'exemple, que la liste des titres des livres achetés sur une librairie en ligne ou des chansons écoutées par une personne concernée sur un service de streaming en ligne sont des données à caractère personnel couvertes par le droit à la portabilité, dès lors qu'elles sont traitées sur la base d'un contrat (Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 8).

[469] Art. 20, § 1er, a), du RGPD.

[470] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 8.

aux 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[471]. Curieusement, l'article 20 du RGPD est cependant muet concernant l'hypothèse dans laquelle le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, ou dans laquelle le traitement est fondé sur l'intérêt légitime du responsable de traitement. Ce mutisme est néanmoins corrigé par les considérants de ce texte, précisant que le droit à la portabilité « ne devrait pas s'appliquer lorsque le traitement est fondé sur un motif légal autre que le consentement ou l'exécution d'un contrat »[472]. Ces deux hypothèses sont donc couvertes par le considérant n° 68. Il eut tout de même été préférable, selon nous, de l'indiquer explicitement dans le texte de l'article 20, paragraphe 3.

Ainsi, le Groupe 29 indique qu'une institution financière n'aura aucune obligation de répondre à une demande de portabilité relative à des données personnelles qui auraient été collectées dans le cadre du respect de son obligation légale de lutte contre le blanchiment d'argent[473].

Pour ce qui est du cas particulier de la relation de travail, et d'une demande de portabilité effectuée par un employé envers son employeur, le Groupe 29 souligne la complexité de la situation, car les traitements effectués par l'employeur seront fondés tantôt sur un contrat ou sur le consentement – considéré par le Groupe 29 comme n'étant, dans nombre de cas, pas donné librement au vu de la relation de subordination[474] –, tantôt sur une obligation légale ou un intérêt légitime supérieur de l'employeur[475]. Une approche au cas par cas s'avèrera donc nécessaire.

Précisons cependant que pour ces catégories de traitements non soumises au droit à la portabilité, le Groupe 29 invite tout de même les responsables de traitements à mettre en œuvre des bonnes pratiques pour répondre rapidement à des potentielles demandes de portabilité, quand bien même n'auraient-ils aucune obligation d'y faire droit, en citant comme exemple la création d'un e-service public proposé par l'administration fiscale et permettant à la personne concernée de télécharger facilement l'ensemble de ses fiches fiscales[476].

---

[471] Article 20, § 3 du RGPD.

[472] Considérant n° 68 du RGPD.

[473] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 8,

[474] Groupe 29, Opinion 8/2001 on the processing of personal data in the employment context, WP 48, 13 September 2001.

[475] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, pp. 8-9.

[476] *Ibid.*, p. 8, note infrapaginale n° 16.

2° Catégories de données auxquelles ce droit s'applique

114. L'article 20, paragraphe 1er, du RGPD dispose qu'en vertu du droit à la portabilité, les personnes concernées ont le droit de recevoir (i) les données à caractère personnel les concernant, (ii) qu'elles ont fournies à un responsable de traitement.

Le texte du RGPD n'apporte pas plus d'éclaircissements dans son article 20, ni dans ses considérants, sur les catégories de données en question, et notamment sur ce qu'il convient d'entendre par des données personnelles « fournies » par la personne concernée. Les lignes directrices du Groupe 29 apportent toutefois un éclairage sur cette question[477].

i. Données à caractère personnel les concernant

115. Cette première partie de la définition des catégories de données auxquelles le droit à la portabilité de l'article 20 du RGPD s'applique n'appelle, à vrai dire, pas d'amples commentaires.

Il convient en effet simplement de souligner que seules les données à caractère personnel sont soumises à ce droit à la portabilité, excluant *de facto* les données non personnelles ainsi que les données originellement personnelles qui ont été anonymisées[478].

En effet, l'anonymisation est définie comme étant le :

> « Processus par lequel des informations personnellement identifiables [IPI] sont altérées de façon irréversible, de sorte que l'individu à qui les IPI ont trait ne peut dorénavant plus être identifié directement ou indirectement, que ce soit par le responsable de traitement des IPI seul, ou avec la collaboration de tout autre tiers [ISO 29100 :2011] »[479].

Dès lors, puisque, au terme du processus d'anonymisation, l'individu n'est plus identifié ou identifiable, il est logique que les données en cause ne soient plus qualifiées de données à caractère personnel, et qu'elles soient, de ce fait, exclues du champ d'application du droit à la portabilité.

---

[477] *Ibid.*, pp. 9-11.

[478] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 9.

[479] Groupe 29, Opinion 05/2014 on Anonymisation Techniques, WP 216, 10 avril 2014, p. 6. Traduction libre de : « *Process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party (ISO 29100 :2011)* ».

116. En revanche, les données personnelles qui ont été simplement pseudonymisées seront bien soumises à ce droit à la portabilité[480]. De fait, la pseudonymisation se définit comme :

> « Le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable »[481].

Ceci justifie donc que, à l'inverse des données anonymisées, les données pseudonymisées soient, pour leur part, couvertes par ce droit à la portabilité, dès lors que la possibilité existe de ré-identifier l'individu auquel ces données ont trait, en ayant recours à des « informations supplémentaires » disponibles par ailleurs. Il s'agit donc toujours de données à caractère personnel, puisque l'individu demeure identifiable.

117. Précisons enfin que, en pratique, nombreuses seront les situations dans lesquelles le responsable de traitement traitera des informations contenant des données à caractère personnel relatives à plusieurs personnes concernées[482]. Dans ces hypothèses, le Groupe 29 invite ces responsables de traitement à ne pas adopter une interprétation exagérément stricte de l'expression « données à caractère personnel les concernant »[483].

À titre d'exemple, le Groupe 29 évoque le cas parlant des relevés téléphoniques ou d'autres systèmes de messagerie interpersonnelle qui peuvent inclure des informations relatives à des tiers avec qui la personne concernée est entrée en communication[484]. Selon le Groupe 29, s'il est vrai que ces relevés peuvent ainsi contenir des données personnelles relatives à des tiers, cela ne devrait pas pouvoir être invoqué par le responsable de traitement, au titre d'une interprétation stricte du RGPD, pour refuser de donner suite à la demande de portabilité de ces relevés introduite par la personne concernée[485]. En revanche, il va de soi que si ces relevés sont ensuite transmis par la personne concernée à un autre responsable de

---

480 Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 9.
481 Art. 4, 5), du RGPD.
482 Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 9.
483 *Ibid.*
484 *Ibid.*
485 Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 9.

traitement, ce dernier devra s'assurer que les traitements qu'il opère sur ces relevés ne porteront pas atteinte aux droits et libertés de ces tiers[486].

ii. Données « fournies » à un responsable de traitement

118. C'est principalement sur cette question de ce qu'il convenait d'entendre par des données « fournies » à un responsable de traitement que les lignes directrices du Groupe 29 s'avèrent être un outil précieux pour la définition du champ d'application du droit à la portabilité.

119. Ainsi, le Groupe 29 identifie trois catégories de données et considère que seules les deux premières d'entre elles doivent être considérées comme étant des données « fournies » à un responsable de traitement, et donc, comme étant soumises au droit à la portabilité[487].

Il s'agit d'une part des « données activement et consciemment fournies par la personne concernée »[488]. Sont ici notamment visées l'adresse email, le nom d'utilisateur, l'âge ou toute autre information qui serait, par exemple, fournie par le biais du remplissage d'un formulaire d'inscription en ligne à un service, à un réseau social, à un site web, etc[489]..

D'autre part, tomberont aussi dans le champ d'application du droit à la portabilité, les « données observées qui sont fournies par la personne concernée par le biais de l'utilisation faite du service ou du produit [du responsable de traitement] »[490].

Citons, à titre d'exemples, l'historique de recherche d'une personne concernée, l'historique des sites web qu'elle aurait visité, les données de trafic et de localisation générées par l'utilisation d'une application mobile, ou encore d'autres types de données brutes, telles que le pouls moyen ou le nombre de pas effectués par une personne concernée, qui seraient collectées par une montre connectée[491]. Dans le même ordre d'idées, nous sommes d'avis que les données résultant d'une analyse de sang – groupe sanguin, taux de globule, etc. – doivent être considérées comme étant collectées à partir de l'utilisation faite, par la personne concernée, du service d'analyse de sang offert par le responsable de traitement.

---

[486] *Ibid.* Sur cette question de la non-atteinte aux droits et libertés des tiers, voy. *infra*, chapitre 1, section 6, § 2, b), 6°.

[487] *Ibid.*, pp. 9-11.

[488] *Ibid.*, p. 10. Traduction libre de : « *data actively and knowingly provided by the data subject* ».

[489] *Ibid.*, pp. 9-10.

[490] *Ibid.*, p. 10. Traduction libre de : « *observed data provided by the data subject by virtue of the use of the service or the device* ».

[491] *Ibid.*

Notons toutefois que l'inclusion, par le Groupe 29, de ces « données observées » dans le champ d'application du droit à la portabilité est critiquée par certains membres de la Commission européenne, qui estiment que ceci pourrait être considéré comme allant au-delà de ce qui a été envisagé par le législateur européen[492]. Ces visions discordantes ne sont pas rassurantes pour les responsables de traitement, qui réclament de la sécurité juridique quant au régime de ce nouveau droit.

120. En revanche, la troisième catégorie de données identifiées par le Groupe 29, à savoir « les données inférées et dérivées [qui] sont créées par le responsable de traitement sur la base de données "fournies par la personne concernée" »[493], ne devront, selon l'avis du Groupe 29, pas être soumises au droit à la portabilité[494]. Sont ici visées les données résultant d'une analyse subséquente réalisée par le responsable de traitement sur la base des données brutes « fournies » (activement ou observées) par la personne concernée[495]. Cela fait sens d'écarter ce type de données, dès lors qu'elles n'ont pas à proprement parler été « fournies » par la personne concernée, mais plutôt « créées » par le responsable de traitement.

Sont notamment visés les profils utilisateurs créés par le responsable de traitement sur la base de l'analyse des données fournies par les personnes concernées, ou encore les résultats d'une évaluation de la santé de la personne concernée fondée sur les données de santé que sa montre intelligente a collectées[496].

Ce seront d'ailleurs bien souvent ces types de données qui auront le plus d'intérêt pour les responsables de traitement, dès lors que c'est là qu'il faut trouver la vraie valeur ajoutée de leur service, de sorte qu'un bon équilibre semble avoir été trouvé entre la préservation des intérêts économiques de ceux-ci et l'objectif de « *data subject empowerment* » qui fonde le droit à la portabilité.

Ceci n'exclut toutefois pas la possibilité pour la personne concernée de faire valoir, à l'égard de ce troisième type de données, son droit d'accès, et plus précisément son droit d'obtenir des informations relatives « à

---

[492] D. Meyer, *European Commission experts uneasy over WP29 data portability interpretation*, 25 April 2017, disponible sur https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation-1/.

[493] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 10. Traduction libre de : « *inferred data and derived data are created by the data controller on the basis of the data "provided by the data subject"* ».

[494] *Ibid.*

[495] *Ibid.*

[496] *Ibid.*

l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée[497] »[498]. Précisons toutefois que les exigences en termes de format dans lequel la personne concernée doit recevoir les données divergent selon que cette transmission fait suite à l'exercice du droit à la portabilité ou du droit d'accès[499].

121. La distinction ainsi effectuée par le Groupe 29 a le mérite d'être claire en théorie, mais suscite deux difficultés en pratique.

D'une part, il ne sera pas nécessairement aisé pour le responsable de traitement de scinder techniquement, dans son système informatique, les deux premières catégories de données de la troisième, en anticipation de l'exercice par une personne concernée du droit à la portabilité.

D'autre part, et ceci accentue d'autant plus la difficulté technique concrète mentionnée ci-dessus, il se peut que, dans certaines situations, il ne soit pas évident de trancher clairement la question de savoir si certaines données ont été « fournies » (activement ou observées) par la personne concernée, ou si, au contraire, ces données auront été « inférées » par le responsable de traitement.

Prenons l'exemple caricatural d'une personne qui, en l'espace d'un mois, effectue plusieurs recherches sur internet afin d'acheter des chaussures de sport bleues, des chemises bleues et des pantalons bleus, car il s'agit là de sa couleur préférée. Sur la base de cet historique, le moteur de recherche que cette personne utilise lui propose une majorité de publicités ayant trait à des vêtements de couleur bleue. À quelle catégorie de données correspond l'information selon laquelle cette personne n'est intéressée que par des vêtements de couleur bleue ? Il ne s'agit vraisemblablement pas de données fournies activement (1re catégorie), car la personne concernée n'a jamais explicitement indiqué que sa couleur préférée était le bleu. Il est, en revanche, moins évident de déterminer si cette information tombe dans la catégorie des « données observées qui sont fournies par la personne concernée par le biais de l'utilisation faite du service ou du produit [du responsable de traitement] »[500] (2e catégorie),

[497] Art. 15, § 1er, h), du RGPD. Voy. *supra*, pt 41.

[498] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 10, note infrapaginale n° 20.

[499] Voy. *infra*, pts 157 et 158 relatifs aux caractéristiques du droit à la portabilité par rapport au droit d'accès.

[500] Groupe 29, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 10. Traduction libre de : « *observed data provided by the data subject by virtue of the use of the service or the device* ».

ou si, au contraire, cette information a été « inférée » par le responsable de traitement sur la base de l'utilisation qui a été faite, par la personne concernée, de son moteur de recherche (3e catégorie).

Dans ce genre de scénarios, le responsable de traitement sera confronté à un choix cornélien : doit-il refuser la portabilité, au risque de violer l'article 20 du RGPD, ou doit-il « porter » les données en cause, au risque de divulguer à ses concurrents une partie de la valeur ajoutée de son service ?

Soulignons à cet égard que le Groupe 29 précise que les termes « données fournies par la personne concernée » doivent être interprétés largement, et englobent « toutes les données personnelles fournies par la personne concernée par le biais de moyens techniques offerts par le responsable de traitement »[501]. En cas de doute sur une catégorie de données, il sera donc conseillé au responsable de traitement de les considérer comme étant couvertes par le droit à la portabilité.

122. En guise de conclusion, l'état de la question, selon les lignes directrices du Groupe 29, peut être résumé comme suit :

> « L'expression "fournies par" recouvre les données personnelles relatives à l'activité de la personne concernée ou résultant de l'observation du comportement d'un individu [2e catégorie], mais n'englobe pas les données résultant de l'analyse subséquente de ce comportement [3e catégorie]. Par contraste, toutes données personnelles qui ont été générées par le responsable de traitement en tant que partie du traitement, par exemple via un processus de personnalisation ou de recommandation par catégorisation ou profilage des utilisateurs, seront considérées comme étant des données dérivées ou inférées à partir des données personnelles fournies par la personne concernée, et ne seront pas couvertes par le droit à la portabilité des données »[502].

---

[501] *Ibid.* Traduction libre de : « *all other personal data provided by the data subject through technical means provided by the controller* ».

[502] *Ibid.*, pp. 10-11. Traduction libre de : « *the term "provided by" includes personal data that relate to the data subject activity or result from the observation of an individual's behaviour, but does not include data resulting from subsequent analysis of that behaviour. By contrast, any personal data which have been generated by the data controller as part of the data processing, e.g. by a personalisation or recommendation process, by user categorisation or profiling are data which are derived or inferred from the personal data provided by the data subject, and are not covered by the right to data portability* ».

b) Principaux éléments constitutifs du droit à la portabilité

123. Après avoir étudié le champ d'application du droit à la portabilité, il convient à présent d'analyser les principaux éléments constitutifs de ce droit.

1° Droit de recevoir les données personnelles

124. Tout d'abord, le droit à la portabilité permet à la personne concernée de recevoir (une partie des) les données à caractère personnel la concernant qu'elle a fournies à un responsable du traitement, et ce, en vue de les stocker pour son propre usage futur, et non dans le but de les transmettre à un autre responsable de traitement[503].

En cette acception, le droit à la portabilité constitue donc plutôt un complément au droit d'accès, en ce sens qu'il permet à la personne concernée de gérer et de réutiliser elle-même les données à caractère personnel la concernant, puisque celles-ci doivent lui être fournies dans un format structuré, couramment utilisé et lisible par machine[504]. Précisons toutefois que les exigences en termes de format ne sont pas identiques pour le droit d'accès[505].

Le Groupe 29 cite ainsi, à titre d'exemple, l'hypothèse dans laquelle la personne concernée désire extraire sa liste de contacts d'une application *Webmail* qu'elle utilise, afin de s'en servir pour construire une liste de mariage[506].

Bien que cet exemple soit parlant, force est toutefois de constater que, en pratique, cette situation spécifique, dans laquelle la personne concernée désirerait elle-même gérer et réutiliser ses données, sans passer par l'intermédiaire d'un service offert par un tiers, se rencontrera peu souvent.

Certes, ceci est imaginable dans des situations, telle que celle mentionnée ci-dessus, où la personne concernée désirerait récupérer une partie limitée des données la concernant. Citons ainsi également le cas d'un journaliste qui exercerait son droit à la portabilité auprès de Twitter, afin de recevoir ses tweets dans un format structuré, couramment utilisé et lisible par machine, dans le but de les réutiliser pour une publication.

Cependant, nous sommes d'avis que, dans la majorité des cas, le droit à la portabilité ne sera pas exercé pour un nombre limité de données, mais

---

503 Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 4.

504 *Ibid.*, p. 5.

505 Voy. *infra*, pts 157 et 158 relatifs aux caractéristiques du droit à la portabilité par rapport au droit d'accès.

506 Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 5.

portera au contraire sur une grande quantité de données. Dans pareille hypothèse, une grande partie des personnes concernées n'auront pas les compétences techniques nécessaires pour faire un usage personnel de ces données.

Imaginons ainsi simplement la situation dans laquelle une personne concernée exercerait, auprès de Google, son droit à la portabilité afin de recevoir toutes les informations que cet opérateur possède à son sujet[507]. Ces nombreuses informations seront fournies sous le format HTML, JSON ou OPML qui, bien qu'étant structurés, couramment utilisés et lisibles par machine, seront vraisemblablement incompréhensibles, en l'état, pour la personne concernée, qui ne saura que faire de toutes les données en question. De fait, ne perdons pas de vue que des données « lisibles par machine » ne seront pas nécessairement « compréhensibles » pour tout qui les consulte, si cette personne ne dispose pas des compétences adéquates.

2° Droit de transmettre, sans obstacle, les données personnelles d'un responsable du traitement à un autre

125. Compte tenu de ce qui a été exposé *supra*, c'est donc la seconde acception du droit à la portabilité qui sera vraisemblablement la plus usitée, à savoir le droit pour la personne concernée de transmettre des données à caractère personnel la concernant d'un responsable de traitement (ci-après le « responsable de traitement originaire ») à un autre (ci-après le « responsable de traitement récipiendaire »), et ce, sans que le responsable de traitement originaire ne puisse y faire obstacle[508].

Dans cette seconde acception, le droit à la portabilité va donc un cran plus loin, en ce sens qu'il permet non seulement à la personne concernée de gérer et de réutiliser les données à caractère personnel la concernant, mais également de les transmettre à un nouveau fournisseur de services, actif dans le même secteur économique ou non[509]. Citons, à titre d'exemple, le « *Data Transfer Project* », né en 2017 et auquel contribuent Google, Facebook,

[507] Le géant américain permet en effet à toute personne titulaire d'un compte Google de télécharger les dites données. Pour ce faire, il suffit pour cette personne de se rendre dans la section « Informations personnelles et confidentialité » de son compte Google, d'ouvrir la sous-section « Définir votre contenu », et de cliquer sur « Télécharger vos données ». Ajoutons que Google contribue, aux côtés notamment de Facebook, Microsoft et Twitter, au « *Data Transfer Project* » né en 2017, dont le but est de créer une plateforme open-source permettant la portabilité directe des données entre les fournisseurs de services participants (voyez https://datatransferproject.dev/).

[508] Art. 20, § 2, du RGPD ; Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 5.

[509] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p.5.

Microsoft et Twitter, dont le but est de créer une plateforme open-source permettant la portabilité directe des données entre les fournisseurs de services participants (https://datatransferproject.dev/).

126. Contrairement à ce que la seule lecture du paragraphe premier de l'article 20 du RGPD pourrait laisser croire, les données en cause ne devront pas nécessairement transiter par la personne concernée[510]. En effet, outre que l'effectivité pratique d'une telle disposition serait quasiment inexistante, puisque ceci exigerait des démarches relativement lourdes de la part de la personne concernée, le second paragraphe de cet article 20 et le considérant n° 68 du RGPD disposent explicitement que :

> « La personne concernée […] a le droit d'obtenir que les données à caractère personnel soient transmises **directement** d'un responsable du traitement à un autre, **lorsque cela est techniquement possible** »[511] (nous soulignons).

C'est notamment dans ce contexte que la recommandation contenue dans le considérant n° 68, mais non dans l'article 20 du RGPD, invitant les responsables de traitement originaires à fournir les données dans un format qui soit non seulement structuré, couramment utilisé et lisible par machine, mais également « interopérable »[512], prend tout son sens.

Ainsi, une telle interopérabilité sera nécessaire pour qu'un responsable de traitement récipiendaire puisse, sur la base du consentement explicite de la personne concernée, recevoir directement les données à caractère personnel de cette personne de la part du responsable de traitement originaire, sans que celles-ci ne transitent par la personne concernée.

---

[510] L'article 20, paragraphe 1er, du RGPD parle en effet du droit pour la personne concernée de « transmettre » les données personnelles la concernant à un autre responsable du traitement, ce qui pourrait être lu comme exigeant implicitement que les données soient d'abord fournies à la personne concernée, afin que celle-ci puisse les transmettre elle-même à cet autre responsable de traitement.

[511] Art. 20, § 2, et consid. 68 du RGPD.

[512] L'interopérabilité est définie comme étant « la capacité de diverses organisations hétérogènes à interagir en vue d'atteindre des objectifs communs, mutuellement avantageux et convenus, impliquant le partage d'informations et de connaissances entre elles, selon les processus d'entreprise qu'elles prennent en charge, par l'échange de données entre leurs systèmes informatiques (TIC) respectifs » (art. 2, 1° de la Proposition de Décision du Parlement européen et du Conseil établissant un programme concernant des solutions d'interopérabilité pour les administrations publiques, les entreprises et les particuliers en Europe (ISA2) – L'interopérabilité comme moyen de moderniser le secteur public, 26 juin 2014, COM/2014/0367 final, disponible sur http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX :52014PC0367&from=FR).

Cependant, étant conscient du fait qu'il serait extrêmement compliqué d'imposer une telle exigence d'interopérabilité aux responsables de traitement originaires, le législateur européen a opté pour la voie de la « simple » recommandation, par le biais du considérant n° 68, plutôt que par le biais de l'intégration d'une référence à l'interopérabilité dans le corps du texte de l'article 20 du RGPD.

127. L'idée sous-jacente de cette seconde acception du droit à la portabilité des données est ainsi de renforcer le « *data subject empowerment* » en évitant des situations de « *lock-in* »[513] et en « générant des opportunités d'innovation et de partage de données personnelles entre des responsables de traitement de façon sécurisée, et sous le contrôle de la personne concernée »[514].

128. Soulignons enfin que le Groupe 29 ne fournit pas d'explications claires sur ce qu'il convient d'entendre par la phrase « lorsque cela est techniquement possible », de l'article 20, paragraphe 2, du RGPD. Or, une telle expression est empreinte d'incertitude juridique.

Selon nous, on peut y voir un renvoi implicite à la notion d'interopérabilité, qui est énoncée dans le considérant n° 68, mais non dans l'article 20 du RGPD, de sorte que les données ne pourraient être transmises directement qu'entre deux systèmes interopérables. Cette vision fait sens sur le plan technique, car si les deux systèmes en cause ne sont pas interopérables, il ne sera probablement pas possible pour le responsable de traitement récipiendaire de recevoir directement les données formatées selon les besoins du responsable de traitement originaire.

Le Groupe 29 semble d'ailleurs partager notre interprétation, ne fût-ce qu'à demi-mot, car, après avoir cité l'article 20, paragraphe 2, du RGPD, les lignes directrices indiquent :

> « À cet égard, le considérant 68 encourage les responsables de traitement à développer des formats interopérables permettant la portabilité »[515].

Le Groupe 29 précise toutefois que, bien que le RGPD interdise aux responsables de traitements d'établir des barrières à la transmission des

---

[513] Voy. pt 109.

[514] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 5. Traduction libre de : « *to foster opportunities for innovation and sharing of personal data between data controllers in a safe and secure manner, under the control of the data subject* ».

[515] *Ibid.* Traduction libre de : « *In this respect, recital 68 encourages data controllers to develop interoperable formats that enable data portability* ».

données, ce texte n'impose pas pour autant aux responsables de traitement de prévoir des systèmes qui soient techniquement compatibles[516].

3° Responsabilité du fait de la portabilité

129. L'une des craintes des responsables de traitement originaires vis-à-vis de la création de ce nouveau droit est le risque pour eux de voir leur responsabilité engagée du fait du traitement opéré par la personne concernée ou par le responsable de traitement récipiendaire sur les données portées.

L'article 20 du RGPD est malheureusement muet sur cette problématique, mais le Groupe 29 a apporté une série de précisions bienvenues.

Ainsi, le Groupe 29 a indiqué que, dans la mesure où le responsable de traitement originaire répond à la demande de portabilité dans le respect des conditions de l'article 20 du RGPD, celui-ci ne pourra pas voir sa responsabilité engagée du fait du traitement opéré sur les données portées par la personne concernée[517] ou par le responsable de traitement récipiendaire desdites données[518].

En effet, le responsable de traitement originaire agit ici pour le compte de la personne concernée, et n'est pas responsable d'une éventuelle absence de conformité du responsable de traitement récipiendaire aux législations protectrices des données à caractère personnel[519]. Selon le Groupe 29, le responsable de traitement originaire devrait tout de même mettre un place certains garde-fous, tels que des procédures internes pour s'assurer de la correspondance entre les données dont la portabilité est demandée et les données effectivement transmises[520].

Par ailleurs, dès lors que l'article 5, paragraphe 1er, d), du RGPD impose au responsable de traitement originaire d'assurer l'exactitude et la mise-à-jour des données, celui-ci ne se voit pas imposer, en vertu du droit à la portabilité, d'obligation additionnelle de vérification de la qualité des données avant d'effectuer le transfert[521].

130. Le responsable de traitement récipiendaire aura, lui, en revanche, l'obligation d'indiquer clairement et directement la finalité du traitement

---

516 *Ibid.*

517 Notons que, bien souvent, le traitement opéré sur les données portées par la personne concernée elle-même sera couverte par l'exception relative au traitement effectué « par une personne physique dans le cadre d'une activité strictement personnelle ou domestique » (art. 2, § 2, c), du RGPD) et sortira du champ d'application du RGPD.

518 Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 6.

519 *Ibid.*

520 *Ibid.*

521 *Ibid.*

qu'il compte opérer avant d'inviter la personne concernée à introduire une demande de portabilité à son profit, et il devra s'assurer que les données portées sont pertinentes et non-excessives au regard de cette finalité[522].

En conséquence, le responsable de traitement récipiendaire n'est pas obligé d'accepter de recevoir et de traiter l'ensemble des données portées, et si celui-ci s'aperçoit que certaines des données portées qu'il a reçues ne sont pas nécessaires à la finalité qu'il poursuit, il devra effacer ces données excédentaires dans les meilleurs délais[523]. À défaut, il pourrait voir sa responsabilité engagée, dès lors qu'il doit être considéré comme étant un nouveau responsable de traitement devant respecter les principes de l'article 5 du RGPD[524].

4° Articulation avec la limitation de la conservation de données à caractère personnel

131. Il convient également de se pencher sur l'articulation de ce droit à la portabilité avec l'obligation qu'a le responsable de traitement de limiter la conservation des données à caractère personnel à une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées[525].

Bien que n'étant pas abordée par l'article 20 du RGPD, cette question épineuse est traitée par le considérant n° 68 du RGPD et par les lignes directrices du Groupe 29.

De fait, le Groupe 29 précise explicitement que :

> « Le droit à la portabilité des données n'impose aucune obligation au responsable de traitement de conserver des données à caractère personnel pour une durée plus longue que ce qui est nécessaire au regard de la finalité ou au-delà de la période de conservation qui a été spécifiée »[526].

Ainsi, ce droit n'impose aucune obligation additionnelle pour le responsable de traitement le contraignant à procéder à la conservation des données à caractère personnel en cause dans le seul but d'être en mesure de répondre à une demande potentielle future de portabilité[527].

---

[522] *Ibid.*, pp. 6-7.
[523] *Ibid.*, p. 6.
[524] *Ibid.*, p. 7.
[525] Art. 5, § 1er, e), du RGPD.
[526] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 6. Traduction libre de : « *Data portability does not impose an obligation on the data controller to retain personal data for longer than is necessary or beyond any specified retention period* ».
[527] *Ibid.*

Le responsable de traitement doit donc permettre la portabilité des données personnelles qu'il conserve pour d'autres finalités, mais il ne doit pas conserver ces données à la seule fin de l'exercice potentiel de ce droit à la portabilité par une personne concernée.

5° Articulation du droit à la portabilité des données avec les autres droits de la personne concernée

132. Afin d'être exhaustif dans notre analyse de la portée du droit à la portabilité, il convient de traiter brièvement de l'articulation de ce droit avec les autres droits de la personne concernée.

Soulignons tout d'abord que, comme pour tout autre droit de la personne concernée, l'exercice, par celle-ci, de son droit à la portabilité est sans préjudice des autres droits accordés par le RGPD à cette personne[528].

À cet égard, il est important de préciser que l'exercice du droit à la portabilité n'implique pas automatiquement l'obligation pour le responsable de traitement d'effacer les données portées[529], l'article 20, paragraphe 3, du RGPD précisant d'ailleurs que l'exercice de ce droit « s'entend sans préjudice de l'article 17 [Droit à l'effacement au sens large] »[530].

Ce faisant, nous sommes d'avis que lorsque l'article 20, paragraphe 1er, du RGPD indique que « les personnes concernées ont le droit de recevoir les données », il convient en réalité de comprendre « les personnes concernées ont le droit de recevoir **une copie des** données » (nous ajoutons). Ceci est d'ailleurs implicitement confirmé par le Groupe 29, qui indique que « ce droit permet aux personnes concernées de déplacer, **copier** ou transmettre plus aisément des données à caractère personnel »[531] (nous soulignons).

Après l'exercice de ce droit à la portabilité, la personne concernée peut, en effet, continuer à vouloir utiliser et bénéficier des services du responsable de traitement originaire auprès de qui il a introduit la demande de portabilité[532].

Il convient donc de constater que, de l'avis le Groupe 29, le droit à la portabilité ne sera pas uniquement utilisé pour quitter un service IT afin d'en utiliser un autre, mais également pour commencer à utiliser un autre

---

528 *Ibid.*, p. 7.

529 *Ibid.*

530 Art. 20, § 3, du RGPD.

531 Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 4. Traduction libre de : « *This right facilitates the ability of data subjects to move, **copy** or transmit personal data easily* ».

532 Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 7.

service IT en « recyclant » des données personnelles déjà fournies à un premier service IT, tout en continuant à utiliser ce premier service.

Nous partageons pleinement cette approche, et sommes d'ailleurs convaincus que ce droit à la portabilité sera majoritairement utilisé dans des hypothèses où la personne concernée désirera continuer à utiliser le service du responsable de traitement originaire. Il n'est donc pas exclu qu'une même personne concernée exerce plusieurs fois son droit à la portabilité à l'égard d'un même responsable de traitement. Ce droit à la portabilité ne doit ainsi pas être uniquement envisagé comme un « one-shot ».

133. Dans le même ordre d'idées, l'exercice par la personne concernée de son droit à la portabilité n'affectera pas la période de conservation originale s'appliquant aux données portées qui aura été définie par le responsable de traitement originaire, et cette personne concernée pourra donc continuer à exercer l'ensemble de ses autres droits reconnus par le RGPD à l'égard du responsable de traitement originaire aussi longtemps que celui-ci continuera de traiter les données portées[533].

134. Enfin, si la personne concernée décide d'exercer son droit à l'effacement au sens large parallèlement à son droit à la portabilité[534], le responsable de traitement ne pourra employer la portabilité comme un moyen de retarder ou de refuser cet effacement[535].

Notons toutefois que, selon nous, si, à l'inverse, la personne concernée exerce son droit à l'effacement au sens large sans jamais avoir exercé son droit à la portabilité au préalable, il ne devrait plus lui être possible d'exercer son droit à la portabilité dans une situation post-effacement, puisque, par hypothèse, le droit à la portabilité des données n'impose aucune obligation au responsable de traitement de conserver des données à caractère personnel, après leur effacement, à la seule fin de l'exercice potentiel futur de ce droit par une personne concernée[536].

6° Non-atteinte aux droits et libertés des tiers

135. Pour conclure cette section relative aux principaux éléments constitutifs du droit à la portabilité, il convient de préciser que l'article 20

---

533 *Ibid.*, p. 7.

534 Imaginons une situation dans laquelle une personne concernée décide de se désinscrire de Facebook et demande à ce réseau social de porter l'ensemble de ses données à caractère personnel vers un nouveau réseau social et, dans le même temps, d'effacer toutes les données à caractère personnel la concernant.

535 Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 7.

536 *Ibid.*, p. 6.

du RGPD prévoit une limitation explicite de ce droit, puisqu'il précise que celui-ci ne peut pas porter atteinte aux droits et libertés des tiers[537].

Cette limitation doit s'envisager à l'égard de deux catégories de données, à savoir, d'une part, les données à caractère personnel d'autres personnes concernées, et, d'autre part, les données protégées au titre des secrets d'affaires ou d'un droit de propriété intellectuelle[538].

i. Données à caractère personnel d'autres personnes concernées

136. Lorsqu'une personne concernée exerce son droit à la portabilité, il conviendra de s'assurer que les données à caractère personnel d'autres personnes concernées, n'ayant pas donné leur consentement à cette portabilité, ne soient pas transmises, par la même occasion, à un responsable de traitement récipiendaire susceptible d'opérer un traitement sur les données personnelles de ces tiers[539]. De fait, si la personne concernée à l'origine de la portabilité a pu donner son consentement au responsable de traitement récipiendaire ou conclure un contrat avec lui, tel n'est pas le cas des autres personnes concernées dont les données pourraient être portées par voie de conséquence[540].

À cet égard, le Groupe 29 nous indique que, dans un tel cas, ce responsable de traitement récipiendaire devra invoquer un autre fondement licite de traitement, tel que l'intérêt légitime de l'article 6, §1er, f) du RGPD, pour pouvoir traiter ces données tierces sans porter atteinte aux droits de ces personnes[541]. Ceci n'est toutefois pas suffisant. En effet, il ne faut pas perdre de vue le principe de finalité de l'article 5, §1er, b) du RGPD, en vertu duquel les données doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne peuvent pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

Or, compte tenu du fait que les tiers en question n'ont pas consenti au transfert des données les concernant vers le responsable de traitement récipiendaire, ce transfert ne pourra avoir lieu que si la finalité pour laquelle ce transfert est réalisé est compatible avec la finalité de départ du responsable de traitement originaire. Tel ne sera généralement pas le cas en pratique. Dans une telle hypothèse, le responsable de traitement devra alors fonder ce nouveau traitement sur une autre base légale que le

[537] Art. 20, § 4, du RGPD.
[538] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, pp. 11-12.
[539] *Ibid.*, p. 11.
[540] *Ibid.*
[541] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 11.

consentement originaire de ces tiers, ou obtenir le consentement de ceux-ci. Enfin, ce responsable de traitement devra informer ces tiers, conformément au prescrit de l'article 14 du RGPD.

137. Afin d'éviter une telle atteinte, le Groupe 29 propose que le traitement des données personnelles de ces autres personnes concernées ne soit autorisé que dans la mesure où ces données demeurent sous le seul contrôle de la personne concernée à l'origine de la portabilité et qu'elles ne soient traitées que pour les seules finalités que cette personne concernée détermine[542]. Le responsable de traitement récipiendaire ne pourrait donc pas traiter ces données tierces pour des finalités qu'il aurait lui-même définies, tel que des finalités de prospection, sous peine de porter atteinte aux droits et intérêts de ces tiers qui n'auront vraisemblablement pas consenti à une telle finalité[543].

Cette proposition fait sens en théorie, mais parait peu convaincante en pratique. Outre qu'elle s'avère être extrêmement restrictive, elle ne présente que peu d'intérêt pour le responsable de traitement récipiendaire, dont la marge de manœuvre sera fortement limitée.

138. Nous sommes, en revanche, plus réceptifs à la seconde proposition du Groupe 29, qui invite tant le responsable de traitement originaire que le responsable de traitement récipiendaire à implémenter des outils techniques permettant à la personne concernée de sélectionner les données à caractère personnel qu'elle souhaite porter, tout en excluant, si possible les données personnelles d'autres personnes concernées[544]. Ceci permet en effet d'éviter, en amont, une potentielle atteinte aux droits de ces tiers.

Cela n'est toutefois pas suffisant en soi, car il n'est pas inimaginable que certaines données personnelles de tiers passent au travers des mailles du filet ou doivent nécessairement être portées.

Il convient donc, en sus de ces outils techniques, de réfléchir à l'implémentation de mécanismes de consentement pour ces autres personnes concernées, afin de faciliter la portabilité des données[545]. À nouveau, se posera la question de la difficile mise en œuvre pratique d'un tel mécanisme, par exemple dans le monde bancaire, où il sera pratiquement impossible d'obtenir le consentement de toutes les personnes apparais-

---

[542] *Ibid.*, p. 12.
[543] *Ibid.*
[544] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 12.
[545] *Ibid.*

sant dans un listing d'opérations bancaires qu'une personne concernée souhaiterait porter vers une autre banque.

ii. Données protégées au titre des secrets d'affaires ou d'un droit de propriété intellectuelle

139. Parallèlement à ce que nous avions déjà souligné *supra*, pour le droit d'accès[546], l'exercice par la personne concernée de son droit à la portabilité pourrait également porter atteinte au secret des affaires ou à la propriété intellectuelle de tiers, qui, au regard des considérants du RGPD[547], sont inclus sous le vocable de droits et libertés d'autrui[548].

Le droit à la portabilité ne peut en effet être utilisé pour commettre des pratiques commerciales déloyales ou pour porter atteinte à un droit de propriété intellectuelle[549]. Le Groupe 29 précise toutefois explicitement qu'un « risque potentiel pour les affaires ne peut toutefois, à lui seul, servir de base pour justifier le refus de donner suite à une demande de portabilité »[550]. Similairement, la violation d'un droit contractuel ne peut être invoquée par le responsable de traitement pour rejeter une demande de portabilité[551].

Une réelle analyse de l'existence d'une atteinte à ces droits doit donc être conduite par le responsable de traitement afin de pouvoir décliner la portabilité pour ce motif.

c) Modalités d'exercice du droit à la portabilité

140. Le dernier élément de notre triptyque de la portée du droit à la portabilité qu'il nous reste à analyser sont les modalités d'exercice de ce droit[552].

---

[546] Voy. pt 44.

[547] Considérant n° 63 du RGPD.

[548] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 12.

[549] *Ibid.*

[550] *Ibid.* Traduction libre de : « *a potential business risk cannot, however, in and of itself serve as the basis for a refusal to answer the portability request* ».

[551] *Ibid.*

[552] L'une des particularités du RGPD, est qu'il régit, en son article 12, les modalités d'exercice de l'ensemble des droits de la personne concernée, en ce compris du droit à la portabilité. Cette disposition est en effet transversale, ce qui explique qu'une section propre lui ait été consacrée dans la présente contribution : voy. *infra*, chapitre 1, section 9. Nous procéderons donc, dans la présente section, majoritairement par renvoi vers ladite section.

1° L'information comme préalable à l'exercice du droit

141. Rappelons tout d'abord que, en vue de faciliter l'exercice par la personne concernée de son droit à la portabilité, le responsable de traitement doit, au préalable, l'informer de l'existence de ce droit[553].

De l'avis du Groupe 29, le responsable de traitement devra, lors de cette information, clairement distinguer le droit à la portabilité des autres droits de la personne concernée, et ce, notamment, en distinguant clairement les catégories de données qui sont couvertes par le droit à la portabilité et celles qui peuvent être obtenues sur la base du droit d'accès[554].

Le Groupe 29 recommande également au responsable de traitement de fournir des informations relatives à la portabilité, à l'expiration du contrat qu'il a conclu avec la personne concernée, de sorte que cette dernière puisse « repartir » avec les données à caractère personnel la concernant[555].

Enfin, le Groupe 29 recommande au responsable de traitement récipiendaire des données portées de fournir une information complète à la personne concernée sur la nature des seules données personnelles qui sont pertinentes pour les finalités qu'il poursuit, et ce, afin de prévenir les risques d'atteinte aux droits et libertés de tiers[556], qui pourraient, par exemple, résulter d'une violation des principes de minimisation des données[557] ou de limitation des finalités de traitement[558].

2° Coût de l'exercice du droit

142. Dans le même objectif de facilitation de l'exercice du droit à la portabilité, le responsable de traitement ne peut demander aucun paiement à la personne concernée pour procéder à toute communication et prendre toute mesure au titre de ce droit, à moins que les demandes de la personne concernée ne soient manifestement infondées ou excessives, notamment en raison de leur caractère répétitif[559].

Le Groupe 29 est d'avis, pour les services de la société de l'information spécialisés dans le traitement automatisé de données à caractère personnel, que

---

[553] Art. 13, § 2, b) et 14, § 2, c), du RGPD.

[554] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 13. Sur cette question, voy. *infra*, pt 158.

[555] *Ibid.*

[556] *Ibid.*

[557] Art. 5, § 1er, c), du RGPD.

[558] Art. 5, § 1er, b), du RGPD.

[559] Art. 12, § 5, du RGPD. Pour plus de précisions sur cette question, voy. *infra*, pt 188.

cette exception sera rarement rencontrée, quand bien même le responsable de traitement serait-il confronté à de multiples demandes de portabilité[560].

En effet, la notion de « caractère répétitif » utilisée dans l'article 12 du RGPD fait référence à des demandes répétées d'une même personne concernée, et non au nombre total de demandes de portabilité que le responsable de traitement pourrait recevoir de la part de plusieurs personnes concernées[561]. Ce faisant, « le coût total de l'implémentation du système ne devrait pas être mis à charge des personnes concernées, ni être utilisé pour justifier un refus de donner suite aux demandes de portabilité »[562].

Par ailleurs, compte tenu du fait que, comme nous l'avons exposé *supra*[563], le droit à la portabilité ne doit pas être uniquement envisagé comme un « one-shot », il nous semble que le « caractère répétitif » de la demande ne doit pas être interprété trop strictement, sous peine de priver ce droit de son effectivité. Ainsi, le simple fait de renouveler une seconde fois la demande de portabilité sur les mêmes données, par exemple pour les transmettre à un troisième responsable de traitement, ne devrait pas suffire à conclure au « caractère répétitif » de la demande. Ce faisant, il conviendra de faire une évaluation au cas par cas du caractère répétitif ou non de la demande, et donc de la possibilité pour le responsable de traitement de réclamer un paiement.

De même, si la personne concernée exerce une nouvelle fois son droit à la portabilité auprès du même responsable de traitement, afin de porter les données mises à jour depuis le premier exercice du droit à la portabilité (nouvelles données, données modifiées, etc.), cette demande ne devrait pas être considérée comme répétitive puisque, par hypothèse, les données portées seront des données différentes de celles ayant été transférées la première fois.

3° Identification de la personne concernée à l'origine de la demande

143. Dans la grande majorité des cas, l'identification de la personne concernée à l'origine de la demande ne posera pas problème.

Si toutefois, au moment de la réception de la demande de portabilité de la personne concernée, le responsable de traitement a des doutes raisonnables quant à l'identité de la personne physique présentant cette demande, il pourra demander que lui soient fournies des informations

---

[560] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 15.

[561] *Ibid.*

[562] *Ibid.* Traduction libre de : « *the overall system implementation costs should neither be charged to the data subjects, nor be used to justify a refusal to answer portability requests* ».

[563] Voy. pt 132.

supplémentaires nécessaires pour confirmer l'identité de cette personne concernée[564]. Cette possibilité de requérir des informations supplémentaires ne peut toutefois justifier des demandes excessives ou la collecte de données qui ne seraient pas pertinentes ou nécessaires pour confirmer l'identité de cette personne concernée[565].

Notons que ce qui précède est « sans préjudice » du cas particulier de l'article 11 du RGPD, que nous avons abordé *supra*[566] et à l'analyse duquel nous nous contentons ici de renvoyer[567].

144. Ajoutons simplement que, pour éviter ces problèmes d'identification, le Groupe 29 encourage les responsables de traitement à mettre en place des procédures d'authentification fondées, par exemple, sur l'utilisation d'un identifiant et d'un mot de passe[568].

4° Délai endéans lequel le responsable de traitement doit traiter la demande

145. Eu égard au texte de l'article 12 du RGPD, qui s'applique de façon transversale à l'ensemble des droits de la personne concernée, une demande de la personne concernée relative à l'exercice du droit à la portabilité doit être traitée « dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande »[569], sauf exception dans des cas plus complexes, où le délai maximal de réponse est de trois mois[570].

Il est important de souligner que le responsable de traitement ne peut rester silencieux et devra obligatoirement réagir dans le temps imparti, quand bien même émettrait-il un refus de procéder à la portabilité[571].

À cet égard, le Groupe 29 invite les responsables de traitement à définir, à l'avance, une période de temps endéans laquelle ils estiment être en mesure de répondre à une demande de portabilité, et à communiquer cette information aux personnes concernées[572].

---

564 Art. 12, § 6, du RGPD.
565 Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 14.
566 Voy. chapitre 1, section 1, § 2, a).
567 Voy. *supra*, pts 27 et 28.
568 Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 14.
569 Art. 12, § 3, du RGPD.
570 Pour plus de précisions sur cette question, voy. *infra*, pts 190 et 191.
571 Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 14.
572 *Ibid.*

Il convient également de préciser que, en présence de responsables conjoints de traitement[573] ou de recours par le responsable de traitement aux services d'un sous-traitant, des procédures spécifiques devront être mises en place, par exemple contractuellement, afin d'assurer qu'il sera répondu, dans les délais prescrits, à la demande de portabilité de la personne concernée[574].

5° Manière dont les données doivent être fournies à la personne concernée

i. Interdiction de faire obstacle juridiquement, techniquement ou financièrement à la portabilité

146. L'article 20 du RGPD stipule que le responsable de traitement originaire ne peut faire obstacle à la portabilité[575]. Selon le Groupe 29, constitue un tel obstacle :

> « Tout obstacle juridique, technique ou financier créé par le responsable de traitement en vue d'empêcher ou de ralentir l'accès, la transmission ou la réutilisation [des données] par la personne concernée ou un autre responsable de traitement »[576].

Sont notamment cités, comme de tels obstacles, des frais excessifs, un manque d'interopérabilité, un délai excessif dans la fourniture des données, ou une standardisation sectorielle excessive[577].

ii. Outils techniques permettant la portabilité

147. Concernant plus précisément la question des outils techniques pouvant être mis en place pour permettre la portabilité, rappelons que l'article 20, paragraphe 2, du RGPD impose aux responsables de traitement de permettre la transmission directe de données à d'autres responsables de traitement « lorsque cela est techniquement possible ».

Cette faisabilité technique doit être évaluée au cas par cas, en tenant compte des considérations évoquées dans le considérant n° 68 du RGPD[578].

---

[573] Art. 26 du RGPD.

[574] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 6.

[575] Art. 20, § 1er, du RGPD.

[576] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 15. Traduction libre de : « *any legal, technical or financial obstacles placed by data controller in order to refrain or slow down access, transmission or reuse by the data subject or by another data controller* ».

[577] *Ibid.*

[578] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 16.

Nous renvoyons, sur ce point, à ce qui a été dit *supra*[579]. En cas d'entraves techniques à une telle transmission directe, le Groupe 29 recommande au responsable de traitement de les expliciter à la personne concernée[580].

148. Si cela s'avère techniquement faisable, deux voies de transmission des données du responsable de traitement originaire vers le responsable de traitement récipiendaire sont envisageables. Soit on recourt à un transfert direct de tout ou partie des données portées, soit on met en place un outil automatisé permettant l'extraction, par le responsable de traitement récipiendaire, des données pertinentes[581].

Le Groupe 29 se montre plutôt favorable à l'utilisation de tels outils automatisés, par exemple une interface de programmation applicative (« API »)[582], dès lors qu'ils permettent de mieux cibler les données pertinentes et de minimiser les risques[583]. Par ailleurs, on pourrait imaginer qu'il soit possible de greffer un mécanisme de synchronisation des données sur ces outils[584].

149. Le Groupe 29 mentionne également la piste intéressante de la création de plateformes de données à caractère personnelles gérées par la personne concernée ou, plus vraisemblablement, par un tiers de confiance, sur lesquelles ces données seraient stockées et à partir desquelles les responsables de traitement pourraient accéder aux et traiter ces données sous le contrôle de la personne concernée, tout en facilitant le transfert de données personnelles d'un responsable de traitement à un autre[585].

Cette proposition n'a rien d'utopique, puisque des projets pilotes de tels systèmes de gestion d'informations personnelles (« PIMS »)[586], existent déjà en Europe, tels que « MiData »[587] au Royaume-Uni et « MesInfos / SelfData »[588] en France.

---

[579] Voy. pt 128.

[580] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 16.

[581] *Ibid.*

[582] Une interface de programmation applicative (API en anglais : « application programming interface ») est défini comme suit : « Il s'agit des interfaces des applications ou des services web qui sont rendus disponibles par les responsables de traitements, afin que d'autres systèmes ou applications puissent se lier à et travailler avec leurs systèmes » (Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 16, note infrapaginale n° 27. Traduction libre de : « *the interfaces of applications or web services made available by data controllers so that other systems or applications can link and work with their systems* »).

[583] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 16.

[584] *Ibid.*

[585] *Ibid.*

[586] « *Personal information management systems* » en anglais.

[587] Voy. https://www.midata.coop/.

[588] Voy. http://mesinfos.fing.org/selfdata/.

Ce second projet est l'œuvre de la Fondation Internet Nouvelle Génération (Fing), et a pour but de renforcer le « *data subject empowerment* », dès lors qu'il vise à promouvoir « la production, l'exploitation et le partage de données personnelles par les individus, sous leur contrôle et à leurs propres fins »[589].

Concrètement, les personnes concernées ont recours à des services tiers de confiance, pouvant se présenter sous la forme de sites web, de plateformes, d'applications ou encore de *Clouds* personnels, sur lesquels les responsables de traitements originaires qui ont accepté de participer au projet partagent, avec le consentement de la personne concernée et au titre du droit à la portabilité, les données à caractère personnel de cette dernière qu'ils traitent[590]. Ceci est avantageux tant pour les personnes concernées, qui peuvent ainsi mieux se connaître, prendre de meilleures décisions, ou encore évaluer leurs décisions passées[591], que pour les responsables de traitements participant au projet, dès lors qu'en échange du partage des données qu'ils détiennent, ceux-ci peuvent, sur la base du consentement de la personne concernée, accéder aux et traiter les données à caractère personnel de cette personne qui ont été partagées par un autre responsable de traitement participant au projet. Il conviendra toutefois, pour chacun de ces responsables de traitement, de s'assurer que les nouveaux traitements ainsi réalisés soient conformes au principe de finalité de traitement[592].

Ce genre d'initiative a le mérite de présenter la portabilité comme étant une opportunité, et non simplement une contrainte, pour les responsables de traitement, et permet de créer de l'interopérabilité.

Il convient toutefois d'être prudent eu égard à la « centralisation » potentielle de données à caractère personnel que peut représenter ce genre d'initiative. En effet, il serait malvenu de rassembler l'ensemble des données à caractère personnel en question dans une seule base de données, aussi sécurisée soit-elle, sous peine de créer un « *Single Point of Failure* » qui pourrait constituer une mine d'or pour des hackeurs voulant s'emparer desdites données à des fins malveillantes. Il est donc impératif de réfléchir à des mécanismes de mise en œuvre technique de ces « espaces personnels de données », que ce soit par le biais de modèles décentralisés de stockage de données tels que les « Banques-Carrefour d'échange de données », ou par le biais d'un découpage virtuel de ces espaces pour chaque personne concernée prise individuellement, de sorte qu'un hackeur ne puisse s'introduire techniquement que sur l'espace personnel d'une personne concernée à la

589 *Ibid.*
590 Voy. http://mesinfos.fing.org/selfdata/.
591 *Ibid.*
592 Art. 5, § 1er, b), du RGPD.

fois, et non en même temps sur l'ensemble de ces espaces personnels, réduisant ainsi l'intérêt – qui ne devient pas nul pour autant – de la démarche pour cette personne aux intentions répréhensibles. À nouveau, il conviendra de s'assurer que les données ne sont pas stockées directement sur l'espace personnel de la personne concernée, sous peine de créer un « *Single Point of Failure* », mais que celles-ci restent stockées auprès de chaque responsable de traitement, qui devrait vérifier la validité de l'identité de la personne demandant la portabilité des données[593], en vue d'éviter les fraudes.

iii. Format de données

150. L'objectif du droit à la portabilité étant de permettre à la personne concernée ou à un autre responsable de traitement de réutiliser les données portées, il est donc essentiel que le format de ces données permette une telle réutilisation[594].

C'est pourquoi l'article 20 du RGPD énonce que les données doivent être transmises « dans un format structuré, couramment utilisé, et lisible par machine[595] »[596]. Le considérant n° 68 du RGPD précise, pour sa part, que le format doit également être « interopérable »[597].

Il convient de ne pas confondre cette notion d'interopérabilité avec la notion de compatibilité, qui n'est, elle, pas exigée dans le cadre du droit

---

[593] Voy. *supra*, pts 143 à 144.

[594] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 16.

[595] Un format lisible par machine est un « format de fichier structuré de telle manière que des applications logicielles puissent facilement identifier et reconnaître des données spécifiques qu'il contient et les en extraire. Les données encodées présentes dans des fichiers qui sont structurés dans un format lisible par machine sont des données lisibles par machine. Les formats lisibles par machine peuvent être ouverts ou propriétaires ; il peut s'agir de normes formelles ou non. Les documents encodés dans un format de fichier qui limite le traitement automatique, en raison du fait que les données ne peuvent pas, ou ne peuvent pas facilement, être extraites de ces documents, ne devraient pas être considérés comme des documents dans des formats lisibles par machine » (consid. 21 de la directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public, *J.O.U.E.*, 27 juin 2013, L 175).

[596] Art. 20, § 1er, du RGPD.

[597] L'interopérabilité est définie comme étant « la capacité de diverses organisations hétérogènes à interagir en vue d'atteindre des objectifs communs, mutuellement avantageux et convenus, impliquant le partage d'informations et de connaissances entre elles, selon les processus d'entreprise qu'elles prennent en charge, par l'échange de données entre leurs systèmes informatiques (TIC) respectifs » (art. 2, 1°, de la Proposition de Décision du Parlement européen et du Conseil établissant un programme concernant des solutions d'interopérabilité pour les administrations publiques, les entreprises et les particuliers en Europe (ISA2) – L'interopérabilité comme moyen de moderniser le secteur public, 26 juin 2014, COM/2014/0367 final, disponible sur http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX :52014PC0367&from=FR).

à la portabilité, puisque le considérant n° 68 du RGPD précise également que ce droit à la portabilité ne devrait pas créer, pour les responsables du traitement, d'obligation d'adopter ou de maintenir des systèmes de traitement qui sont techniquement compatibles[598].

151. Au-delà de ces exigences, le RGPD n'impose pas de recommandations spécifiques quant au format devant être utilisé, ceci étant laissé à l'appréciation des responsables de traitement, qui doivent néanmoins garder à l'esprit qu'il est souhaitable que le format choisi permette l'interopérabilité[599]. Ce faisant, il sera bon d'éviter de recourir à des formats soumis à des contrats de licence couteux, et d'envisager, au contraire, des formats ayant un haut degré d'abstraction[600]. Ceci invite à opérer le choix de formats ouverts/libres couramment utilisés (tels que le format XML, JSON ou CSV) aux dépens de formats propriétaires[601].

152. Notons que ce processus de sélection, d'extraction et d'adaptation en un format adéquat des données à caractère personnel qui feront l'objet de la portabilité implique la réalisation d'une série de traitements par le responsable, qui devraient être considérés comme étant compatibles avec les finalités du traitement annoncées originellement par ce responsable de traitement[602].

153. Le Groupe 29 invite également les responsables de traitement à fournir des métadonnées[603] aussi précises et exhaustives que possible avec les données portées, et ce, au meilleur niveau de granularité possible, afin de décrire au mieux la signification de ces données portées[604].

Ceci s'inscrit à plein dans la volonté qu'a le législateur européen de faciliter la réutilisation des données portées, au même titre que l'invitation faite aux responsables de traitement de proposer, si possible, plusieurs types de formats à la personne concernée tout en lui expliquant

---

598 Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 17.

599 *Ibid.*

600 *Ibid.*

601 *Ibid.*, p. 18.

602 *Ibid.*, p. 18.

603 Une métadonnée est une « information décrivant [des données] et rendant possible leur recherche, leur inventaire et leur utilisation » (art. 3, 6) de la directive 2007/2/CE du Parlement européen et du Conseil du 14 mars 2007 établissant une infrastructure d'information géographique dans la Communauté européenne (INSPIRE), *J.O.C.E.*, 25 avril 2007, L 108).

604 Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 18.

clairement les conséquences s'attachant au choix de l'un ou l'autre de ces formats[605].

154. Enfin, le Groupe 29 « encourage fortement la coopération entre les acteurs de l'industrie et les associations professionnelles aux fins d'établir ensemble une série de standards et de formats interopérables en vue de satisfaire aux exigences du droit à la portabilité »[606]. Selon le Groupe 29, ces acteurs pourraient, pour ce faire, s'inspirer du Cadre Européen d'Interopérabilité[607], qui établit une série d'éléments communs en matière de vocabulaire, de concepts, de principes, de politiques, de lignes directrices, de recommandations, de standards, de spécifications et de pratiques[608].

De notre avis, cette coordination afin de mettre en œuvre ces standards d'interopérabilité aura de plus grandes chances d'aboutir si elle est organisée au niveau sectoriel, puisque ceci permet d'avoir un nombre raisonnable de partenaires autour de la table. En effet, plus le nombre d'acteurs impliqués dans la discussion est important, plus il sera compliqué de parvenir à un accord. Qui plus est, la portabilité aura vraisemblablement le plus souvent lieu au sein d'un même secteur d'activités[609] (la personne concernée désire changer de banque, d'opérateur téléphonique, de réseau social, etc.).

iv. Cas particulier de la portabilité d'une masse vaste et complexe de données personnelles

155. Comme expliqué ci-dessus, la finalité de la portabilité est de permettre à la personne concernée de réutiliser les données portées, ce qui ne sera pas toujours aussi simple qu'il n'y parait, notamment lorsque la personne concernée sera confrontée à une masse vaste et complexe de données à caractère personnel, puisque, en ce cas, il y a fort à parier que

---

[605] *Ibid.*

[606] *Ibid.* Traduction libre de : « *strongly encourages cooperation between industry stakeholders and trade associations to work together on a common set of interoperable standards and formats to deliver the requirements of the right to data portability* ».

[607] Disponible uniquement en anglais (European Interoperability Framework) sur http://eur-lex.europa.eu/resource.html?uri=cellar :2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_3&format=PDF.

[608] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 18.

[609] Il faut toutefois reconnaitre que le droit à la portabilité a également vocation à s'exercer entre secteurs d'activités distincts. En ces cas, le développement de standards sectoriels d'interopérabilité ne suffira pas. Cependant, il nous parait peu réaliste d'imaginer qu'un seul standard d'interopérabilité, commun à tous les secteurs, puisse voir le jour.

cette personne ne sera pas en mesure de pleinement saisir la définition, le schéma et la structure des données qui lui sont ainsi fournies[610].

C'est notamment en ces hypothèses que l'idée, émise par le Groupe 29, de permettre à un tiers de confiance d'accéder, pour le compte de la personne concernée et avec son consentement, aux données détenues par le responsable de traitement par le biais d'un API[611], peut s'avérer intéressante[612].

De fait, ceci pourrait offrir une forme d'accès plus sophistiquée au système d'information du responsable de traitement originaire, qui permettrait aux personnes concernées de « découper » leurs demandes de portabilité, ainsi que de réclamer uniquement la portabilité des données qui n'ont pas été modifiées depuis leur dernière demande[613].

v. Sécurisation des données

156. Comme le souligne l'article 5, paragraphe 1er, f), du RGPD, le responsable de traitement doit :

> « Garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ».

En matière de portabilité des données, le responsable de traitement originaire devra principalement mettre en œuvre toutes les mesures de sécurité nécessaires pour s'assurer que les données à caractère personnel portées sont transmises de façon sécurisée à la bonne personne, sans pour autant que ces mesures ne constituent un obstacle, notamment financier, à l'exercice par la personne concernée de son droit à la portabilité[614].

Dans cette optique, le responsable de traitement « devrait évaluer les risques spécifiques liées à la portabilité des données et prendre les mesures appropriées de mitigation de ces risques »[615]. Sont notamment suggérées des mesures d'authentification (additionnelles) – notamment via l'utilisation de *tokens* – ou de suspension ou de gel de la transmission en cas de suspicion de fraude[616].

---

610 Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 18.
611 Voy. *supra*, pts 148 et 149.
612 Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 18.
613 *Ibid.*, p. 19.
614 *Ibid.*
615 *Ibid.* Traduction libre de : « *should assess the specific risks linked with data portability and take appropriate risks mitigation measures* ».
616 *Ibid.*

De même, le responsable de traitement originaire est invité à sensibiliser la personne concernée récipiendaire des données portées à l'importance de stocker celles-ci dans un système informatique sécurisé, et ce, par exemple, en lui recommandant des formats et des mesures de sécurité appropriées, par exemple des mesures de cryptage[617].

d) Caractéristiques du droit à la portabilité par rapport au droit d'accès

157. Compte tenu du fait que le droit d'accès contient à présent explicitement le droit d'obtenir une copie des données[618], il convient de se questionner sur la pertinence de l'insertion d'un nouveau droit à la portabilité dans le RGPD. À notre sens, cette insertion se justifie sur trois plans.

Tout d'abord, il ne faut pas perdre de vue que, là où le droit d'accès a comme seul but d'assurer le « *data subject empowerment* », à savoir le renforcement du contrôle et du droit à l'autodétermination informationnelle de la personne concernée, le droit à la portabilité des données a, en plus de cet objectif, également un second objectif qui est de renforcer la concurrence dans le marché numérique en évitant le « *consumer lock-in* »[619]. Se pose toutefois la question de la pertinence de traiter une question de droit de la concurrence dans un texte visant à assurer la protection des données à caractère personnel.

Ensuite, et ceci est lié à ce qui précède, le droit à la portabilité devrait faciliter le transfert des données puisque, lorsque cela est techniquement possible, celui-ci peut s'opérer directement entre les deux responsables de traitement, sans que la personne concernée ne doive, elle-même, recevoir les données en transit, cette dernière devant simplement donner son consentement à l'opération[620]. Le droit d'accès, à l'inverse, ne permet pas cette transmission directe. Ceci est plus efficace que si la personne concernée devait, dans un premier temps, demander une copie de toutes les données la concernant via le droit d'accès, pour ensuite, dans un deuxième temps, les faire parvenir au second responsable de traitement. Ce type de mécanismes de transfert direct entre responsables de traitement permet ainsi, notamment, d'implémenter des plateformes de type « SelfData »[621].

Enfin, le droit à la portabilité des données implique des exigences de format de données plus strictes (« format structuré, couramment utilisé et

617 *Ibid.*
618 Voy. *supra*, pts 42 à 46 relatifs à l'article 15, § 3, du RGPD.
619 Voy. *supra*, pt 109.
620 Art. 20, § 2, du RGPD.
621 Voy. *supra*, pt 149.

lisible par machine »[622]) que le droit d'accès (« sous une forme électronique d'usage courant »[623]). Or, le format utilisé est déterminant pour faciliter la réutilisation des données. Ainsi, un fichier PDF sera vraisemblablement considéré comme rencontrant la condition de « forme électronique d'usage courant »[624], mais il ne permettra pas à la personne concernée ou au second responsable de traitement d'en extraire aisément les données afin de les réutiliser pour un autre service. En effet, la référence à un « format structuré, couramment utilisé et lisible par machine »[625] implique, selon nous, que les données à caractère personnel y contenues devraient pouvoir en être extraites techniquement, sans devoir recopier les données en cause dans un nouveau fichier. Nous pensons ainsi que les formats CSV ou JSON satisfont à cette exigence.

C'est précisément là l'intérêt du droit à la portabilité, qui est envisagé comme un outil technique de réutilisation des données. Bien souvent, les données portées seront incompréhensibles, en l'état, pour la personne concernée. De fait, ne perdons pas de vue que des données « lisibles par machine » ne seront pas nécessairement « compréhensibles » pour tout qui les consulte, si cette personne ne dispose pas des compétences adéquates. Ceci témoigne d'une différence fondamentale avec le droit d'accès, qui ne vise pas à permettre la réutilisation technique des données dont la personne concernée a obtenu une copie, mais bien à lui permettre de comprendre les traitements réalisés sur les données la concernant, afin de pouvoir exercer un contrôle sur ses données, dans une perspective d'autodétermination informationnelle.

158. Concluons cette brève section en rappelant que le champ d'application du droit à la portabilité des données est cependant plus réduit que le champ d'application du droit d'accès. En effet, le droit d'accès s'applique à toutes les données à caractères personnel traitées par le responsable de traitement, quel que soit le fondement légitime de ces traitements[626]. En revanche, en vertu de l'article 20, paragraphe 1er, du RGPD, le droit à la portabilité s'applique uniquement aux données personnelles « fournies » (activement ou observées) par la personne concernée – et non aux données « inférées » par le responsable de traitement –[627], et dont le

[622] Article 20, § 1er du RGPD.
[623] Article 15, § 3 du RGPD.
[624] *Ibidem*.
[625] Article 20, § 1er du RGPD.
[626] Art. 15 du RGPD.
[627] Voy. *supra*, pts 118 à 122.

traitement est fondé sur le consentement de la personne concernée ou sur un contrat[628].

§ 3. Articulation de l'article 20 du RGPD avec d'autres matières du droit traitant de la portabilité

159. Bien que ce droit à la portabilité des données à caractère personnel soit une nouveauté en matière de protection des données, « d'autres types de portabilité existent déjà ou sont en train d'être discutées dans d'autres domaines du droit (par ex. en matière de terminaison de contrats, de roaming de services de communications ou d'accès transfrontalier à des services) [et] certaines synergies et même certains bénéfices pour les individus pourraient émerger entre ces différents types de portabilité si elle sont fournies via une approche combinée, bien que ces possibles analogies doivent être envisagées avec précaution »[629]. Ainsi, le concept de portabilité fait également son apparition en matière de droit de la concurrence et de droit de la protection des consommateurs.

160. Le Groupe 29 attire d'ailleurs l'attention sur la problématique d'un potentiel cumul de droits à la portabilité, puisque certaines législations sectorielles spécifiques ou législations de protection des consommateurs, tant nationales qu'européennes, pourraient également consacrer des formes de droit à la portabilité[630].

En pareil cas, le Groupe 29 invite le responsable de traitement à déterminer si l'intention de la personne concernée est d'exercer son droit à la portabilité sous l'empire du RGPD et/ou d'une de ces autres législations, l'article 20 du RGPD ne s'appliquant pas, selon le Groupe 29, si la personne concernée entend uniquement exercer son droit à la portabilité sous l'empire de ces autres législations[631]. Selon nous, il convient d'être précis sur ce que le Groupe 29 soutient dans cette hypothèse particulière. Le Groupe 29 indique ainsi que c'est uniquement la disposition spécifique du RGPD relative au droit à la portabilité qui ne trouvera pas à s'appliquer, ce qui n'exclut nullement l'application de tout autre article perti-

---

628 Voy. *supra*, pts 112 à 113.

629 Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 4. Traduction libre de : « *other types of portability already exist or are being discussed in other areas of legislation (e.g. in the contexts of contract termination, communication services roaming and trans-border access to services). Some synergies and even benefits to individuals may emerge between these types of portability if they are provided in a combined approach, even though analogies should be treated cautiously* ».

630 *Ibid.*, p. 7.

631 *Ibid.*, p. 8.

nent du RGPD[632], si tout ou partie des données portées en vertu de ces autres législations s'avèrent être des données à caractère personnel.

Si, en revanche, la personne concernée entend exercer son droit à la portabilité sous l'empire de l'article 20 du RGPD conjointement avec le droit à la portabilité reconnu par une autre de ces législations, il conviendra de procéder à une articulation méticuleuse au cas par cas des principes de l'article 20 du RGPD avec les autres dispositions invoquées, ces dernières ne pouvant toutefois pas supplanter les principes de l'article 20 du RGPD[633].

a) Droit de la concurrence

161. La question de la portabilité des données est tout d'abord traitée en droit de la concurrence, ce qui n'a rien d'étonnant, dès lors que l'un des deux objectifs poursuivis par l'inclusion de ce nouveau droit dans le RGPD est de permettre à la personne concernée de pouvoir passer plus facilement d'un fournisseur de service à un autre, ce qui devrait avoir pour conséquence de renforcer la concurrence en matière de services en ligne, en facilitant la création de nouveaux services[634].

Ainsi, en droit de la concurrence, se pose la question de savoir si la limitation de la portabilité de données pourrait être constitutive d'un abus de position dominante, au sens de l'article 102 du TFUE[635].

Ceci pourrait notamment résulter d'un risque « d'enfermement »[636] des consommateurs, ce qui a été invoqué par plusieurs opérateurs télécoms en vue de s'opposer à la fusion entre Facebook et Whatsapp[637] :

> « Plusieurs opérateurs télécoms ont indiqué que des coûts de changement d'opérateur pourraient se matérialiser, pour les consommateurs, par la perte de toutes leurs données et de tout leur historique d'interaction lorsque ceux-ci changent d'application de communication »[638].

---

[632] Nous pensons notamment aux articles 5 (Principes relatifs au traitement des données à caractère personnel) et 6 (Licéité du traitement) du RGPD, dont le respect devra être assuré en toute hypothèse.

[633] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 8.

[634] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 4. Voy. *supra*, pts 107 à 109.

[635] I. Graef, *EU competition law, data protection and online platforms : data as essential facility*, Alphen aan den Rijn, Kluwer, 2016, p. 147.

[636] « Lock-in ».

[637] I. Graef, *EU competition law, data protection and online platforms : data as essential facility*, *op. cit.*, p. 147.

[638] Commission européenne, Décision de non-opposition à la fusion entre Facebook et WhatsApp, affaire M.7217, § 113 (uniquement disponible en anglais). Traduction libre de : « *Several telecom operators indicated that switching costs for consumers would be represented by the loss of all data and interaction history when changing consumer communications app* ».

Notons toutefois que, dans le cas d'espèce, la Commission n'a pas suivi cet argument et a avalisé la fusion[639]. Le second risque créé par une limitation de la portabilité des données est celui de l'exclusion de concurrents, ce qui a notamment eu pour conséquence que, dans l'affaire qui l'oppose actuellement à la Commission européenne[640], le géant américain Google ait dû s'engager à supprimer les limitations faites à la portabilité des campagnes de publicité faites originairement sur AdWords[641].

162. S'il est vrai qu'il existe un certain parallèle en matière de portabilité entre le droit de la concurrence et le droit de la protection des données, trois différences doivent toutefois être soulignées[642].

Tout d'abord, la portabilité est consacrée, dans le RGPD, sous la forme d'un droit pour la personne concernée, alors qu'elle est envisagée sous forme d'obligation pour l'entreprise en droit de la concurrence[643].

Ensuite, la portabilité est limitée, dans le RGPD, aux données à caractère personnel « fournies » par la personne concernée[644], tandis qu'elle s'applique potentiellement à tous types de données – qu'elles soient personnelles ou non – en droit de la concurrence[645].

Enfin, le droit à la portabilité sous l'empire du RGPD s'applique à tout traitement de données à caractère personnel effectué à l'aide de procédés automatisés et se fondant sur le consentement de la personne concernée ou sur un contrat conclu avec celle-ci[646], tandis que la portabilité est limitée, en droit de la concurrence, aux cas particuliers et individuels d'atteintes au droit de la concurrence[647].

b) Droit de la protection des consommateurs

163. La problématique de la portabilité des données est également évoquée en droit de la protection des consommateurs. Une nouvelle fois, ceci ne surprend pas, dès lors que le second objectif poursuivi par l'inclusion

---

[639] Commission européenne, Décision de non-opposition à la fusion entre Facebook et WhatsApp, affaire M.7217, § 191 (uniquement disponible en anglais).

[640] *Commission européenne c. Google*, affaire AT.39740.

[641] I. Graef, *EU competition law, data protection and online platforms : data as essential facility*, *op. cit.*, p. 144.

[642] *Ibid.*, pp. 332-335.

[643] *Ibid.*, p. 334.

[644] Voy. *supra*, pts 118 à 122.

[645] I. Graef, *EU competition law, data protection and online platforms : data as essential facility*, *op. cit.*, p. 334.

[646] Voy. *supra*, pts 112 et 113.

[647] I. Graef, *EU competition law, data protection and online platforms : data as essential facility*, *op. cit.*, p. 334.

d'un tel droit dans le RGPD est de « "rééquilibrer" la relation entre les personnes concernées et les responsables de traitements »[648], et ce, « au travers de l'affirmation des droits personnels et du contrôle des individus sur les données à caractère personnel les concernant »[649], soit un objectif de « *data subject empowerment* »[650], qui s'inscrit dans la mouvance actuelle plus large du « *consumer empowerment* ».

164. Ainsi, en droit de la protection des consommateurs, une certaine forme de portabilité est consacrée dans l'article 13 de la proposition de directive concernant certains aspects des contrats de fourniture de contenu numérique, qui dispose que :

> « Lorsque le consommateur résilie le contrat :
> b) le fournisseur prend toutes les mesures attendues pour **s'abstenir d'utiliser la contrepartie non pécuniaire** que le consommateur a apportée en échange du contenu numérique **et toutes autres données qu'il a collectées dans le cadre de la fourniture du contenu numérique, y compris tout contenu fourni par le consommateur**, à l'exception des contenus générés conjointement par le consommateur et d'autres personnes qui continuent à en faire usage ;
> c) le fournisseur procure au consommateur les moyens techniques lui permettant de **récupérer tout contenu fourni par ce dernier et toutes autres données produites ou générées par suite de l'utilisation du contenu numérique par le consommateur**, dans la mesure où ces données ont été conservées par le fournisseur. Le consommateur a le **droit de récupérer le contenu gratuitement, sans inconvénient majeur, dans un délai raisonnable et dans un format de données couramment utilisé** »[651] (nous soulignons).

L'article 16 de cette proposition de directive est également pertinent, en ce qu'il dispose que :

> « Lorsque le consommateur résilie le contrat conformément au présent article :
> a) le fournisseur prend toutes les mesures attendues pour **s'abstenir d'utiliser la contrepartie non pécuniaire** que le consommateur a

[648] Groupe 29, Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017, p. 4. Traduction libre de : « *by affirming individuals' personal rights and control over the personal data concerning them* ».

[649] *Ibid.* Traduction libre de : « *represents an opportunity to "re-balance" the relationship between data subject and data controllers* ».

[650] Voy. *supra*, pts 107 à 109.

[651] Art. 13, § 2, b) et c), de la Proposition de directive du Parlement européen et du Conseil concernant certains aspects des contrats de fourniture de contenu numérique, 9 décembre 2015, COM(2015) 634 final.

apportée en échange du contenu numérique **et toutes autres données collectées par le fournisseur dans le cadre de la fourniture du contenu numérique, y compris tout contenu fourni par le consommateur** ;
b) le fournisseur procure au consommateur les moyens techniques lui permettant de **récupérer tout contenu fourni par ce dernier et toutes autres données produites ou générées par suite de l'utilisation du contenu numérique par le consommateur**, dans la mesure où ces données ont été conservées par le fournisseur. Le consommateur a le **droit de récupérer le contenu sans inconvénient majeur, dans un délai raisonnable et dans un format de données couramment utilisé** » (nous soulignons)[652].

165. À l'analyse, il s'avère que le régime de portabilité qui serait créé par ces deux dispositions, si le texte de la proposition de directive était adopté en l'état, diverge sur quatre plans par rapport au régime de la portabilité de l'article 20 du RGPD.

Premièrement, les champs d'application de ces deux régimes ne sont pas identiques, en ce qu'ils couvrent des types de données différentes. Ainsi, si le régime de l'article 20 du RGPD couvre uniquement des données à caractères personnel fournies directement ou indirectement[653] par la personne concernée, à l'exclusion des données personnelles inférées par le responsable de traitement[654], le régime de la proposition de directive s'applique à « tout contenu fourni par ce dernier et toutes autres données produites ou générées par suite de l'utilisation du contenu numérique par le consommateur[655] »[656]. Sont ainsi visées, dans la proposition de directive, tant des données personnelles que des données non personnelles. Concernant la question des données « inférées » par le responsable de traitement / fournisseur, le libellé de la proposition de directive ne nous permet pas de déterminer si elles sont également couvertes. En effet, le terme « contenu fourni par [le consommateur] » n'est pas défini dans le texte de la proposition. Or, si le terme « fourni » devait être interprété, pour la proposition, tel qu'il est

[652] Art. 16, § 4, a) et b), de la Proposition de directive du Parlement européen et du Conseil concernant certains aspects des contrats de fourniture de contenu numérique, 9 décembre 2015, COM(2015) 634 final.

[653] Via l'utilisation du service.

[654] Voy. *supra*, pts 118 à 122.

[655] Art. 13, § 2, b) et c) et 16, § 4, a) et b), de la Proposition de directive du Parlement européen et du Conseil concernant certains aspects des contrats de fourniture de contenu numérique, 9 décembre 2015, COM(2015) 634 final.

[656] I. Graef, *EU competition law, data protection and online platforms : data as essential facility*, *op. cit.*, p. 148.

interprété par le Groupe 29, pour l'article 20 du RGPD, il ne nous semblerait pas invraisemblable de considérer que ces données « inférées » puissent également être couvertes par le régime de la proposition de directive, sous le vocable de « autres données produites ou générées par suite de l'utilisation du contenu numérique », ces données étant, à première vue, distinctes des données « fournies », directement ou indirectement, par le consommateur. Il est, toutefois, également envisageable que les « autres données produites ou générées par suite de l'utilisation du contenu numérique » correspondent, en réalité, aux données « observées » de l'article 20 du RGPD, de sorte que les données « inférées » ne seraient pas non plus couvertes par le texte de la proposition de directive.

Deuxièmement, le droit à la portabilité de l'article 20 du RGPD permet, en théorie, la transmission directe des données entre les responsables de traitement originaire et récipiendaire, sans que la personne concernée ne doive, elle-même, recevoir les données en transit, cette dernière devant simplement donner son consentement à l'opération[657]. Le régime de portabilité de la proposition de directive, à l'inverse, ne permet pas cette transmission directe[658], puisqu'elle vise uniquement à consacrer le droit pour le consommateur de récupérer personnellement les données[659]. La proposition se rapproche, en ce sens, plutôt du droit d'accès contenu dans le RGPD, qui permet d'obtenir une copie des données personnelles[660]. Concernant les conséquences pratiques que cette distinction engendre, nous nous contentons ici de renvoyer à ce qui a été dit au sujet de la comparaison entre le droit à la portabilité et le droit d'accès sur ce point, dès lors que ces propos sont transposables à la présente comparaison[661].

Troisièmement, le droit à la portabilité des données de l'article 20 du RGPD implique des exigences de format de données plus strictes (« format structuré, couramment utilisé et lisible par machine »[662]) que le droit à la portabilité de la proposition de directive (« format de données couramment utilisé »[663]). À nouveau, la proposition se rapproche, en ce sens,

[657] Art. 20, § 2, du RGPD.

[658] I. Graef, *EU competition law, data protection and online platforms : data as essential facility*, *op. cit.*, p. 148.

[659] Art. 13, § 2, c) et 16, § 4, b), de la Proposition de directive du Parlement européen et du Conseil concernant certains aspects des contrats de fourniture de contenu numérique, 9 décembre 2015, COM(2015) 634 final.

[660] Art. 15, § 3, du RGPD.

[661] Voy. *supra*, pt 157.

[662] Art. 20, § 1er, du RGPD.

[663] Art. 13, § 2, c) et 16, § 4, b), de la Proposition de directive du Parlement européen et du Conseil concernant certains aspects des contrats de fourniture de contenu numérique, 9 décembre 2015, COM(2015) 634 final.

plutôt de l'exigence de format requise pour le droit d'accès (« sous une forme électronique d'usage courant »[664]), et implique donc les mêmes différences en termes de conséquences pratiques, auxquelles nous nous contentons, à nouveau, de renvoyer[665].

Quatrièmement, le sort des données détenues par le responsable de traitement originaire / fournisseur de service suite à l'exercice du droit à la portabilité diffère dans les deux régimes. Ainsi, si en vertu de l'article 20 du RGPD, le responsable de traitement peut continuer à traiter les données portées si la personne concernée n'en a pas demandé l'effacement concomitant[666], tel n'est pas le cas du fournisseur dans le régime de la proposition de directive. En effet, cette proposition indique que le fournisseur doit s'abstenir d'utiliser, à l'avenir, les données fournies par le consommateur ainsi que toutes autres données collectées par le fournisseur dans le cadre de la fourniture du contenu numérique[667]. Cette divergence de régime s'explique, en réalité, par le fait que la portabilité peut s'exercer à tout moment dans le RGPD, tandis qu'elle n'est envisagée que suite à la résiliation du contrat de fourniture du contenu numérique dans la proposition de directive[668].

En revanche, ces régimes semblent être alignés sur la question de la gratuité de la portabilité[669] et du délai dans lequel il doit être donné suite à cette demande de portabilité. Nous pensons en effet que le délai d'un mois évoqué dans le RGPD[670] pourrait être utilisé pour évaluer le caractère raisonnable du délai évoqué dans la proposition de directive[671].

Au vu de ce qui précède, il nous paraitrait souhaitable, dans la version finale de cette directive concernant certains aspects des contrats de fourniture de contenu numérique, d'aligner le régime de portabilité sur celui de l'article 20 du RGPD, afin d'éviter des situations complexes de cumul de portabilités, qui pourraient mener à des insécurités juridiques.

---

[664] Art. 15, § 3, du RGPD.

[665] Voy. *supra*, pt 157.

[666] Voy. *supra*, pt 132.

[667] Art. 13, § 2, b) et c) et 16, § 4, a) et b), de la Proposition de directive du Parlement européen et du Conseil concernant certains aspects des contrats de fourniture de contenu numérique, 9 décembre 2015, COM(2015) 634 final.

[668] I. Graef, *EU competition law, data protection and online platforms : data as essential facility*, *op. cit.*, p. 148.

[669] Art. 12, § 5, du RGPD et art. 13, § 2, c) et 16, § 4, b), de la Proposition de directive du Parlement européen et du Conseil concernant certains aspects des contrats de fourniture de contenu numérique, 9 décembre 2015, COM(2015) 634.

[670] Art. 12, §§ 3 et 4, du RGPD.

[671] Art. 13, § 2, c) et 16, § 4, b), de la Proposition de directive du Parlement européen et du Conseil concernant certains aspects des contrats de fourniture de contenu numérique, 9 décembre 2015, COM(2015) 634.

166. Précisons, par ailleurs, que la portabilité des données n'est pas le seul mécanisme envisagé au niveau européen pour lutter contre le « risque d'enfermement » des consommateurs et pour favoriser le « *consumer empowerment* ». Ainsi, dès 2005, cette volonté s'est traduite dans la directive sur les pratiques commerciales déloyales[672] :

> « Afin de déterminer si une pratique commerciale recourt au harcèlement, à la contrainte, y compris la force physique, ou à une influence injustifiée, les éléments suivants sont pris en considération :
> d) **tout obstacle non contractuel** important ou disproportionné **imposé** par le professionnel **lorsque le consommateur souhaite faire valoir ses droits contractuels, et notamment celui** de mettre fin au contrat ou **de changer** de produit ou **de fournisseur** »[673] (nous soulignons).

167. Enfin, précisons que le droit de la protection des consommateurs pourra s'avérer être un remède salvateur pour les consommateurs, dès lors qu'il n'est pas soumis aux limites inhérentes du droit de la protection des données et du droit de la concurrence. Son champ d'action est donc fort large.

168. En conclusion, il sera donc non seulement indispensable pour les responsables de traitement de respecter le prescrit de l'article 20 du RGPD relatif à la portabilité des données à caractère personnel, mais également de veiller à se conformer aux règles adoptées, en matière de portabilité de données, en droit de la concurrence et en droit de la protection des consommateurs.

[672] Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) 2006/2004 du Parlement européen et du Conseil (« directive sur les pratiques commerciales déloyales »), *J.O.U.E.*, 11 juin 2005, L 149.

[673] Art. 9, d), de la directive 2005/29/CE sur les pratiques commerciales déloyales.

SECTION 7. – Droit d'opposition (article 21 du RGPD)

169. La personne concernée bénéficie également du droit de s'opposer, dans certaines situations que nous exposerons *infra*, au traitement de ses données à caractère personnel par le responsable de traitement[674].

L'article 21, paragraphe 4, du RGPD rappelle d'ailleurs que, comme exposé dans nos développement relatifs au droit de la personne concernée

[674] Art. 21 du RGPD. Ce droit d'opposition était déjà consacré à l'article 14 de la Directive.

d'être informée du traitement[675], l'existence de ce droit doit être explicitement portée à l'attention de la personne concernée, et ce, au plus tard au moment de la première communication avec celle-ci[676]. Ceci était déjà prévu dans la Directive[677], mais le RGPD va un pas plus loin, en ajoutant que cette information doit être présentée « clairement et séparément de toute autre information »[678], ce qui illustre bien la volonté qui habite le texte du RGPD d'augmenter la transparence à l'égard des personnes concernées.

170. À titre liminaire, il convient d'attirer l'attention sur une confusion trop souvent commise en pratique. Ce droit d'opposition doit en effet bien être distingué du droit pour la personne concernée de rétracter le consentement qu'elle aurait donné au responsable de traitement afin de légitimer un traitement effectué par ce dernier[679]. Ce droit de rétractation du consentement ne relève en effet pas du droit d'opposition, mais plutôt de l'article 7 du RGPD, relatif aux conditions applicables au consentement, qui dispose que la personne concernée a le droit de retirer son consentement à tout moment, ce retrait devant être aussi aisé que la fourniture dudit consentement[680].

Le droit d'opposition s'avèrera, pour sa part, particulièrement pertinent lorsque le traitement effectué par le responsable de traitement ne repose pas sur un tel consentement de la personne concernée, puisque, en pareil cas, le responsable du traitement aura, de sa propre initiative, estimé que le traitement qu'il effectue trouve son fondement sur un motif de licéité de traitement autre que le consentement[681], et ce, sans prendre en compte l'avis de la personne concernée[682]. Par le biais de ce droit d'opposition, la personne concernée se voit ainsi reconnaitre le droit de remettre en cause cette décision unilatérale du responsable de traitement.

Précisons au sujet de l'exercice de ce droit d'opposition que la personne concernée peut, dans le cadre de l'utilisation de services de la société de

---

675 Voy. *supra*, pt 17, art. 13, § 2, b), du RGPD et pt 23, art. 14, § 2, c), du RGPD.

676 Art. 21, § 4, du RGPD.

677 Art. 14, al. 2, de la Directive.

678 *Ibid.*

679 C. DE TERWANGNE, « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », *op. cit.*, p. 108.

680 Art. 7, § 3, du RGPD.

681 Art. 6, § 1er, b) à f), du RGPD.

682 C. DE TERWANGNE, « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », *op. cit.*, p. 107.

l'information[683] exercer son droit d'opposition à l'aide de procédés automatisés utilisant des spécifications techniques[684].

§ 1. Droit d'opposition au traitement fondé sur l'article 6, paragraphe 1er, e) ou f), du RGPD, y compris un profilage fondé sur ces dispositions

171. La personne concernée a, tout d'abord, le droit de s'opposer, à tout moment et pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant, qui est nécessaire aux fins des intérêts légitimes poursuivis par le responsable de traitement ou par un tiers prévalant sur les intérêts, droits et libertés fondamentaux de la personne concernée, ou qui 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 de traitement[685].

Comme le souligne la professeure C. de Terwangne :

> « Ce droit est particulièrement important dans les hypothèses où le responsable a effectué lui-même, *a priori*, la mise en balance des intérêts en présence et a estimé que le résultat était équilibré et qu'il pouvait légitimement traiter les données »[686].

Cela fait, en effet, sens de permettre, dans un tel cas, à la personne concernée de remettre en cause le résultat de la mise en balance ainsi opérée par le responsable de traitement[687]. Notons que le RGPD contient, sur ce point, un apport majeur par rapport à la Directive, puisque la tâche de la personne concernée a été facilitée sur deux plans.

D'une part, s'il est vrai que la personne concernée doit toujours faire montre d'un certain intérêt légitime pour pouvoir exercer son droit d'opposition dans l'hypothèse susvisée, « l'intensité » de l'intérêt requis a été revu à la baisse. Ainsi, là où la Directive prévoyait que la personne concernée devait faire valoir des « raisons **prépondérantes et légitimes** tenant à sa situation

---

683 Un service au sens de l'article 1er, § 1er, b), de la directive 2015/1535/UE du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information, *J.O.U.E.*, 17 septembre 2015, L 241.

684 Art. 21, § 5, du RGPD.

685 Art. 21, § 1er, du RGPD. L'article 14, al. 1er, a), de la Directive était formulé de façon analogue.

686 C. DE TERWANGNE, « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », *op. cit.*, p. 107.

687 *Ibid.*, p. 108.

particulière »[688], le RGPD exige simplement aujourd'hui que celle-ci justifie sa demande sur la base de « raisons tenant à sa situation particulière »[689].

D'autre part, la charge de la preuve a été renversée[690], et il appartient désormais au responsable de démontrer qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts, droits et libertés fondamentaux de la personne concernée[691].

172. Il peut, à l'inverse, paraître plus curieux de reconnaitre à la personne concernée le droit de s'opposer à un traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement. De fait, est-il bien légitime de permettre à un individu de faire prévaloir ses intérêts personnels sur l'intérêt général ? En réalité, il existe des situations dans lesquelles la possibilité d'exercer ce droit d'opposition est pleinement justifiée.

Citons ainsi l'exemple d'une jeune afghane qui avait fui son pays et sa famille, en vue d'échapper à un mariage forcé. Celle-ci, une fois arrivée en Belgique, s'était inscrite dans l'une des universités du pays. En vue d'assurer sa mission de service public de délivrance de diplômes professionnalisants, l'université dispense des cours, dont certains sont assortis de travaux pratiques, pour lesquels les étudiants sont répartis en différents groupes. Afin de permettre aux étudiants de savoir à quel groupe ils appartenaient, ces listes étaient publiquement accessibles sur internet.

Se rendant compte que ceci pouvait mettre sa vie en danger, puisque en faisant une recherche fondée sur son nom, sa famille aurait pu savoir où elle se trouvait, l'étudiante afghane a exercé son droit d'opposition à l'encontre de l'université, afin de voir son nom retiré des listes publiques. En pareil cas, on comprend aisément que l'exercice du droit d'opposition de la personne concernée est justifié, quand bien même le traitement en cause serait-il nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement. Ce dernier point est d'ailleurs discutable, car il n'est pas certain que la diffusion publique sur internet de ces listes était nécessaire.

---

688 Art. 14, al. 1er, a), de la Directive.

689 Art. 21, § 1er, du RGPD.

690 Ce renversement de la charge de la preuve a également été intégré dans le projet de modernisation de la Convention 108 (C. DE TERWANGNE, « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », *op. cit.*, p. 108).

691 Art. 21, § 1er, du RGPD.

Une autre voie moins attentatoire, telle que la diffusion via un intranet, aurait pu être envisagée.

Un autre exemple parlant est celui de la diffusion en ligne de la jurisprudence de la Cour européenne des droits de l'homme ou de la Cour de justice de l'Union européenne. En principe, ces décisions contiennent le nom des parties, ce qui est justifié au regard de l'exercice de l'autorité publique dont ces juridictions sont investies, mais les personnes concernées peuvent s'y opposer et requérir l'anonymisation des décisions.

173. La personne concernée dispose également du droit de s'opposer, à tout moment et pour des raisons tenant à sa situation particulière, au profilage reposant sur les deux fondements de traitement exposés ci-dessus[692].

Pour rappel, le RGPD définit le profilage comme étant :

> « 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 »[693].

Ceci est révélateur d'un autre cheval de bataille du RGPD, à savoir la promotion du droit à l'autodétermination informationnelle de la personne concernée, qui désire comprendre la logique sous-jacente des traitements dont elle fait l'objet et qui la catégorisent sous tel ou tel profil[694].

174. Lorsque, dans les trois hypothèses visées ci-dessus, la personne concernée a exercé son droit d'opposition avec succès, le responsable de traitement ne pourra plus traiter les données à caractère personnel en cause, à moins qu'il ne démontre que ce traitement est nécessaire à la constatation, l'exercice ou la défense de droits en justice[695].

Ajoutons que la Directive ne précisait pas si, en de telles hypothèses, le responsable de traitement était en droit de réclamer un paiement auprès

---

692 Art. 21, § 1er, du RGPD.

693 Art. 4, 4), du RGPD.

694 Sur ces questions de volonté de compréhension de la logique sous-jacente des traitements automatisés et du droit à l'autodétermination informationnelle, voy. *supra*, pt 41 de la présente contribution, ainsi que C. DE TERWANGNE, « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », *op. cit.*, pp. 105-108.

695 Art. 21, § 1er, du RGPD.

de la personne concernée qui exerçait son droit d'opposition. Le RGPD ne contient pas non plus une telle précision en son article 21 relatif au droit d'opposition.

Cependant, il convient rappeler l'existence de l'article 12, paragraphe 5, du RGPD, qui régit de façon commune les modalités d'exercice de l'ensemble des droits de la personne concernée[696], et qui dispose qu'aucun paiement ne peut être exigé pour prendre toute mesure au titre du droit d'opposition, à moins que la demande de la personne concernée ne s'avère manifestement infondée ou excessive[697].

Précisons, enfin, que l'article 12, paragraphe 3, du RGPD dispose qu'une demande de la personne concernée relative à l'exercice de ce droit doit être traitée « dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande »[698], sauf exception[699].

§ 2. Droit d'opposition au traitement réalisé à des fins de prospection, y compris en cas de profilage lié à une telle prospection

175. La personne concernée dispose, par ailleurs, du droit de s'opposer, à tout moment, et sans aucune justification, au traitement des données à caractère personnel la concernant, lorsque ces données sont traitées à des fins de prospection[700], en ce compris en cas de profilage lié à une telle prospection[701].

L'hypothèse visée ici est celle dans laquelle le responsable traite des données à caractère personnel à des fins de « *marketing direct* » ou à des fins de générer des profils afin de cibler plus précisément ses efforts de « *marketing direct* », auquel cas la personne concernée peut s'opposer à ce traitement **sans aucune justification**[702].

---

[696] Sur cette question des modalités d'exercice de l'ensemble des droits de la personne concernée, voy. chapitre 1, section 9.

[697] Art. 12, § 5, du RGPD. Pour plus de précisions sur cette question, voy. *infra*, pt 188.

[698] Art. 12, § 3, du RGPD

[699] Pour plus de précisions sur cette question, voy. *infra*, pts 190 et 191.

[700] Ceci était également prévu à l'article 14, al. 1er, b), de la Directive.

[701] Art. 21, § 2, du RGPD.

[702] À la différence des autres hypothèses dans lesquelles un droit d'opposition est reconnu à la personne concernée, puisque, en ces cas, celle-ci doit invoquer des « raisons tenant à sa situation particulière » (voy. art. 21, §§ 1er et 4, du RGPD, ainsi que chapitre 1, section 7, § 1 et chapitre 1, section 7, § 3 de cette contribution).

De façon assez surprenante, la disposition correspondante de la Directive était plus loquace que le RGPD sur cette question.

D'une part, la Directive prévoyait explicitement que ce droit d'opposition était gratuit[703]. L'article du RGPD relatif au droit d'opposition, pour sa part, ne traite pas explicitement de la question, ce qui peut paraitre curieux, dès lors que le considérant n° 70 du RGPD précise que ce droit d'opposition au traitement réalisé à des fins de prospection doit être « sans frais ».

En réalité, il conviendra ici de se référer à l'article 12 du RGPD, qui traite, par souci d'effectivité, des modalités d'exercice de l'ensemble des droits de la personne concernée. Cet article dispose qu'aucun paiement ne peut être exigé pour prendre toute mesure au titre du droit d'opposition, à moins que la demande de la personne concernée ne s'avère manifestement infondée ou excessive[704], et qu'une demande de la personne concernée relative à l'exercice de ce droit doit être traitée « dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande »[705], sauf exception[706].

D'autre part, la Directive octroyait à la personne concernée le droit d'être informée avant que des données à caractère personnel ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection et de se voir expressément offrir le droit de s'opposer, gratuitement, à ladite communication ou utilisation[707]. Force est de constater que, de façon assez surprenante, ce droit n'a pas été repris dans le RGPD, et ce, sans que l'on sache s'il s'agit simplement là d'un oubli, ou d'un choix délibéré.

§ 3. Droit d'opposition au traitement réalisé à des fins de recherche scientifique ou historique ou à des fins statistiques

176. Enfin, le RGPD prévoit que la personne concernée a le droit de s'opposer, pour des raisons tenant à sa situation particulière, au traitement de données à caractère personnel la concernant, lorsque des données à caractère personnel sont traitées à des fins de recherche scientifique ou historique ou à des fins statistiques en application de l'article 89,

[703] Art. 14, al. 1er, b), de la Directive.
[704] Art. 12, § 5, du RGPD. Pour plus de précisions sur cette question, voy. *infra*, pt 188.
[705] Art. 12, § 3, du RGPD
[706] Pour plus de précisions sur cette question, voy. *infra*, pts 190 et 191.
[707] Art. 14, al. 1er, b), de la Directive.

paragraphe 1er, du RGPD, à moins que le traitement ne soit nécessaire à l'exécution d'une mission d'intérêt public[708].

Une nouvelle fois, le RGPD a atténué « l'intensité » de l'intérêt requis dans le chef de la personne concernée, celle-ci devant simplement justifier sa demande sur la base de « raisons tenant à sa situation particulière »[709], et non plus faire valoir des « raisons prépondérantes et légitimes tenant à sa situation particulière »[710]. Par ailleurs, le RGPD procède, à nouveau, à un renversement de la charge de la preuve, puisqu'il appartient au responsable de démontrer que le traitement en cause est nécessaire à l'exécution d'une mission d'intérêt public.

De plus, et conformément à l'article 12 du RGPD, l'exercice de ce droit d'opposition est gratuit, à moins que la demande de la personne concernée ne s'avère manifestement infondée ou excessive[711], et la demande de la personne concernée relative à l'exercice de ce droit doit être traitée « dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande »[712], sauf exception[713].

§ 4. Absence de droit d'opposition pour certaines catégories de traitements

177. Concluons en mettant en exergue que, dès lors que l'article 21 du RGPD ne fait aucunement mention des hypothèses de traitements nécessaires au respect d'une obligation légale à laquelle le responsable de traitement est soumis[714] ou à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique[715], il convient d'en déduire que la personne concernée ne se voit pas, en pareil cas, octroyer de droit d'opposition.

Il en va de même pour les traitements nécessaires à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci[716], pour autant que ceux-ci ne soient pas conclus à des fins de prospection.

---

708 Art. 21, § 6, du RGPD.
709 Art. 21, § 4, du RGPD.
710 Art. 14, al. 1er, a), de la Directive.
711 Art. 12, § 5, du RGPD. Pour plus de précisions sur cette question, voy. *infra*, pt 188.
712 Art. 12, § 3, du RGPD
713 Pour plus de précisions sur cette question, voy. *infra*, pts 190 et 191.
714 Art. 6, § 1er, c), du RGPD.
715 Art. 6, § 1er, d), du RGPD.
716 Art. 6, § 1er, b), du RGPD.

Enfin, soulignons qu'il est étonnant que l'article 21 du RGPD ne fasse aucunement mention de la possibilité de s'opposer aux traitements de données sensibles visées aux articles 9 et 10 du RGPD. De fait, si, comme analysé *supra*, la personne concernée peut s'opposer au traitement de certaines données « ordinaires » traitées sur la base de l'article 6 du RGPD, il paraitrait logique que celle-ci puisse également s'opposer au traitement de certaines données sensibles – et risquant donc d'engendrer des conséquences plus graves pour cette personne – lorsque cela s'avèrerait justifié. Il s'agit vraisemblablement là d'un oubli malencontreux du législateur européen.

SECTION 8. – Droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé (art. 22 du RGPD)

§ 1. Portée du droit

178. Le dernier droit qu'il nous reste à traiter dans le présent chapitre, est le droit pour la personne concernée de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage[717], produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire[718].

À titre d'exemple, le RGPD mentionne le rejet automatique d'une demande de crédit en ligne ou des pratiques de recrutement en ligne sans aucune intervention humaine comme étant des traitements affectant de manière significative la personne concernée[719].

179. Ce droit fait écho à la volonté forte qu'a l'être humain de ne pas être intégralement soumis à la machine, celui-ci n'acceptant pas l'idée qu'une décision puisse lui être imposée sur la seule base de conclusions

[717] Profilage : « 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 » (art. 4, 4), du RGPD).

[718] Art. 22, § 1er, du RGPD. Ce droit était déjà consacré par l'article 15 de la Directive.

[719] Considérant n° 71 du RGPD.

auxquelles cette machine serait parvenue[720]. Comme l'indique la professeure C. de Terwangne, « c'est là l'expression de la prééminence à accorder à la dignité humaine »[721].

Précisons d'ailleurs que cette intrication forte entre promotion de la dignité humaine et droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé était déjà intrinsèque à la Directive, puisque l'article 15 de celle-ci, pendant de l'article 22 du RGPD, était inspiré de l'article 1er de la loi française du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, qui stipulait, dans sa version en vigueur au moment de l'adoption de la Directive que :

> « L'informatique doit être au service de chaque citoyen. […] Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques »[722].

Notons également que la volonté de mettre en avant cette valeur fondamentale qu'est la dignité humaine ne ressort pas uniquement du RGPD, mais également, à plus forte raison, de la Convention 108 modernisée, puisque le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé est présenté comme étant le premier droit de la personne concernée[723], et qu'une référence explicite à la nécessité de garantir la dignité humaine a été insérée dans le préambule de cette Convention 108 modernisée[724].

Cet ajout dans le préambule de la Convention 108 modernisée met d'ailleurs également en exergue un autre droit fondamental de la personne concernée, que nous avons déjà mentionné à plusieurs reprises

---

[720] C. de Terwangne, « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », *op. cit.*, p. 104.

[721] *Ibid.*

[722] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 1er.

[723] Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), adoptée à Elseneur (Danemark) les 17 et 18 mai 2018, CM/Inf(2018)15-final, art. 9, § 1er, a).

[724] « Considérant qu'il est **nécessaire de garantir la dignité humaine** ainsi que la protection des droits de l'homme et des libertés fondamentales de toute personne **et**, eu égard à la diversification, à l'intensification et à l'internationalisation des traitements de données et des flux de données à caractère personnel, **l'autonomie personnelle, fondée sur le droit de la personne de contrôler ses propres données à caractère personnel et le traitement qui en est fait** » (Préambule de la Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), adoptée à Elseneur (Danemark) les 17 et 18 mai 2018, CM/Inf(2018)15-final).

dans le présent chapitre[725], à savoir le droit à l'autodétermination informationnelle de cette personne, qui lui permet de contrôler ses propres données à caractère personnel et le traitement qui en est fait[726].

180. Cette volonté de remettre l'humain au cœur du débat est d'autant plus pertinente à l'heure où, en raison du développement numérique, la tendance grandissante est de « s'en remettre à un "ordinateur" et aux algorithmes qu'il applique pour décider du traitement à réserver à un individu »[727].

Ainsi, il ressort des conclusions d'une étude réalisée par LRDP Kantor Ltd que :

> « Face à la multiplication des analyses de plus en plus automatisées de données toujours plus nombreuses et accessibles, les individus risquent d'être réduits à de simples objets qui seront traités […] sur la base de "profils" informatiques, de probabilités et de prévisions, sans possibilité de s'opposer aux algorithmes sous-jacents. À défaut de maintenir une protection des données très stricte, les décisions qui ont un "impact significatif" seront de plus en plus motivées "par le fait que l'ordinateur a dit non" »[728].

Cet article 22 du RGPD aura donc un rôle prépondérant à jouer dans les années à venir, au regard du développement des « *Big data* » et des activités concomitantes de profilage.

§ 2. Exceptions spécifiques assorties de garanties appropriées, notamment le droit d'obtenir une explication

181. Le principe exprimé ci-dessus est toutefois assorti d'exceptions spécifiques. Ainsi, la prise de décision fondée exclusivement sur

---

[725] Voy. *supra*, pts 41 et 42 (Droit d'accès), 98 (Droit à l'oubli), 108 (Droit à la portabilité) et 173 (Droit d'opposition).

[726] Préambule de la Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), adoptée à Elseneur (Danemark) les 17 et 18 mai 2018, CM/Inf(2018)15-final.

[727] C. DE TERWANGNE, « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », *op. cit.*, p. 104.

[728] LRDP Kantor Ltd, en association avec Centre for Public Reform, *Étude comparative sur les différentes approches des nouveaux défis en matière de protection de la vie privée, en particulier à la lumière des évolutions technologiques*, Rapport final, Note de synthèse, disponible sur http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_fr.pdf, janvier 2010, pp. 21-22, cité par C. DE TERWANGNE, « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », *op. cit.*, p. 104.

un traitement automatisé, y compris le profilage, devrait être permise lorsqu'elle est :

– Nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement[729] ; ou
– Autorisée par le droit de l'Union ou le droit d'un État membre auquel le responsable du traitement est soumis[730], et qui prévoit également des mesures appropriées pour la sauvegarde des droits, libertés et intérêts légitimes de la personne concernée[731] ; ou
– Fondée sur le consentement explicite de la personne concernée[732].

Le RGPD précise que dans les cas où la prise de décision est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement, ou est fondé sur le consentement explicite de la personne concernée, le responsable du traitement se doit de mettre en œuvre des mesures appropriées pour la sauvegarde des droits, libertés et intérêts légitimes de la personne concernée[733].

Un parallèle est donc fait ici avec la prise de décision autorisée par le droit de l'Union ou le droit d'un État membre, à la différence que, cette fois, ce n'est pas le législateur, mais bien le responsable de traitement lui-même qui doit mettre en œuvre ces garanties appropriées.

Devront à tout le moins faire partie de ces garanties appropriées, les droits pour la personne concernée d'obtenir une intervention humaine de la part du responsable de traitement, d'exprimer son point de vue, et de contester la décision[734].

182. Soulignons toutefois que le considérant n° 71 du RGPD va un cran plus loin, dès lors qu'il consacre également, au titre de garantie appropriée minimale devant être mise en œuvre au profit de la personne concernée, le droit de recevoir une information spécifique relative à ces garanties et le droit d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation[735]. Assez curieusement, ces deux droits n'ont pas été incorporés dans l'article 22, paragraphe 3, du RGPD.

---

[729] Art. 22, § 2, a), du RGPD.

[730] Le considérant n° 71, alinéa 1er, du RGPD fait notamment référence aux législations adoptées aux fins de contrôler et de prévenir les fraudes et l'évasion fiscale, et d'assurer la sécurité et la fiabilité d'un service fourni par le responsable du traitement.

[731] Art. 22, § 2, b), du RGPD.

[732] Art. 22, § 2, c), du RGPD.

[733] Art. 22, § 3, du RGPD.

[734] *Ibid.*

[735] Considérant n° 71, al. 1er, du RGPD.

Selon certains auteurs, cela implique que l'article 22 du RGPD ne consacre, en réalité, pas le droit d'obtenir une explication quant à la décision fondée exclusivement sur un traitement automatisé[736], dès lors qu'un considérant seul, n'a pas force de loi[737]. Pour ces auteurs, il ne s'agit pas d'une simple omission, mais bien d'une volonté réelle de ne pas inclure ce droit dans le texte de l'article 22, paragraphe 3, du RGPD[738]. Le Parlement européen avait en effet proposé d'inclure ce droit dans l'article du RGPD[739], tandis que le Conseil était d'avis de ne mentionner ce droit que dans les considérants[740], ce qui démontre bien que le texte final du RGPD résulte d'un choix délibéré posé durant le trilogue, et non d'une simple erreur de rédaction[741].

Ces auteurs admettent toutefois qu'il pourrait être soutenu que « bien que cela ne soit certainement pas explicite dans le phrasé de l'article 22, § 3, le droit d'obtenir une intervention humaine de la part du responsable de traitement, d'exprimer son point de vue ou de contester une décision serait inutile si la personne concernée ne peut pas comprendre comment la décision contestée a été prise »[742]. Ainsi, ce droit d'obtenir une explication quant à la décision fondée exclusivement sur un traitement automatisé pourrait être contenu en germe dans cet article 23, paragraphe 3, du RGPD.

Cette piste semble confirmée par le rapport explicatif de la Convention 108 modernisée qui précise que :

---

[736] Voy. S. WACHTER, B. MITTELSTADT et L. FLORIDI, « Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation », *International Data Privacy Law*, vol. 7, n° 2, 2017, pp. 76-99.

[737] *Ibid.*, p. 80.

[738] S. WACHTER, B. MITTELSTADT et L. FLORIDI, « Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation », *op. cit.*, p. 81.

[739] Amendement n° 115 du Rapport de la Commission des libertés civiles, de la justice et des affaires intérieures sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), 22 novembre 2013, A7-0402/2013 – 2012/0011(COD), disponible sur http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2013-0402+0+DOC+XML+V0//FR.

[740] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) – Préparation d'une orientation générale, Présidence du Conseil de l'Union européenne, 11 juin 2015, 9565/15, consid. 58 et art. 20, § 1b.

[741] S. WACHTER, B. MITTELSTADT et L. FLORIDI, « Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation », *op. cit.*, p. 81.

[742] *Ibid.*, p. 91. Traduction libre de : « *although it is certainly not explicit in the phrasing of Article 22(3), the right to obtain human intervention, express views or contest a decision is meaningless if the data subject cannot understand how the contested decision was taken* ».

> « Les personnes concernées [...] ont le droit d'obtenir connaissance de la logique sur laquelle repose le traitement de leurs données et qui aboutit à la décision [...] au lieu d'être simplement informés de la décision elle-même. La compréhension de ces éléments contribue à l'exercice effectif d'autres garanties essentielles comme le droit d'opposition et le droit de recours auprès de l'autorité compétente »[743].

Le Groupe 29 tient un discours semblable, en indiquant que « le responsable de traitement devrait trouver des façons simples d'exprimer à la personne concernée le raisonnement ou les critères employés pour aboutir à la décision »[744] et que l'information ainsi fournie devrait être « suffisamment complète pour que [cette personne] puisse comprendre les motifs de la décision »[745]. De fait, pour le Groupe 29, « la personne concernée sera uniquement en mesure de contester une décision ou d'exprimer son point de vue si elle comprend pleinement comment elle a été prise et sur quelle base »[746].

De surcroît, il nous semble que ce droit d'obtenir une explication est également intrinsèquement inclus dans le droit à l'information de la personne concernée[747], ainsi que dans le droit d'accès de celle-ci[748]. Ces deux droits lui permettent, en effet, de recevoir des informations utiles concernant la logique sous-jacente du traitement qui la concerne, qui, nous l'avons vu[749], devrait non seulement permettre à la personne concernée de savoir ce qui se passe avec ses données, mais aussi de comprendre la logique sous-tendant le traitement[750]. Il n'empêche qu'il eût été préférable, par souci de clarté, d'intégrer explicitement la référence à ce droit d'obtenir une explication dans l'article 22, paragraphe 3, du RGPD.

---

[743] Rapport explicatif du Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) – Convention 108 modernisée, CM(2018)2-addfinal, pt 77.

[744] Groupe 29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251 rev.01, 6 February 2018, p. 25. Traduction libre de : « *The controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision* ».

[745] *Ibid.* Traduction libre de : « *sufficiently comprehensive for the data subject to understand the reasons for the decision* ».

[746] *Ibid.*, p. 27. Traduction libre de : « *The data subject will only be able to challenge a decision or express their view if they fully understand how it has been made and on what basis* ».

[747] Art. 13, § 2, f) et 14, § 2, g), du RGPD.

[748] Art. 15, § 1er, h), du RGPD.

[749] Voy. *supra*, pt 41.

[750] C. DE TERWANGNE, « La réforme de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », *op. cit.*, p. 107.

183. Ajoutons que le considérant n° 71 du RGPD précise également que les exceptions spécifiques, dont question ci-avant, ne devraient pas pouvoir concerner des enfants[751], ce qui est totalement absent du texte de l'article 22 du RGPD. La valeur contraignante de cette affirmation est donc, somme toute, limitée.

184. Le considérant n° 71 du RGPD invite par ailleurs, dans son second alinéa, le responsable de traitement à assurer un traitement équitable et transparent à l'égard de la personne concernée, et contient, dans cette optique, les recommandations suivantes :

> « Le responsable du traitement devrait utiliser des procédures mathématiques ou statistiques adéquates aux fins du profilage, appliquer les mesures techniques et organisationnelles appropriées pour faire en sorte, en particulier, que les facteurs qui entraînent des erreurs dans les données à caractère personnel soient corrigés et que le risque d'erreur soit réduit au minimum, et sécuriser les données à caractère personnel d'une manière qui tienne compte des risques susceptibles de peser sur les intérêts et les droits de la personne concernée et qui prévienne, entre autres, les effets discriminatoires à l'égard des personnes physiques fondées sur l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions, l'appartenance syndicale, le statut génétique ou l'état de santé, ou l'orientation sexuelle, ou qui se traduisent par des mesures produisant un tel effet »[752].

À première vue, ces recommandations semblent avoir une valeur contraignante limitée, étant donné qu'elles ne sont pas reprises dans le texte de l'article 22 du RGPD. En réalité, ces recommandations ne sont que la formulation d'obligations contraignantes formulées ailleurs dans le RGPD, à savoir le principe de « *privacy by design* »[753] (mesures techniques et organisationnelles appropriées), l'exigence de qualité des données[754] (réduction du risque d'erreurs et correction des erreurs), et l'exigence de sécurisation des données[755] (sécurisation tenant compte des risques pour les personnes concernées).

185. Enfin, il convient de mentionner les décisions spécifiques visées à l'article 22, paragraphe 2, du RGPD ne peuvent être fondées sur les catégories particulières de données à caractère personnel visées à l'article 9,

---

751 Considérant n° 71, al. 1er, du RGPD.
752 Considérant n° 71, al. 2, du RGPD.
753 Art. 25 du RGPD.
754 Art. 5, § 1er, d), du RGPD.
755 Art. 5, § 1er, f), du RGPD.

paragraphe 1er[756], à moins que l'article 9, paragraphe 2, a)[757] ou g)[758], ne s'applique et que des mesures appropriées pour la sauvegarde des droits, libertés et intérêts légitimes de la personne concernée ne soient mises en place[759].

§ 3. Exercice du droit

186. Pour conclure, étant donné que les modalités de l'exercice de ce droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé ne sont pas contenues dans l'article 22 du RGPD relatif à ce droit, mais dans l'article 12 du RGPD, qui régit de façon commune les modalités d'exercice de l'ensemble des droits de la personne concernée[760], nous invitons le lecteur à se référer à l'analyse de ces modalités effectuée *infra*[761].

Précisons simplement, à ce stade, que cet article 12 dispose qu'une demande de la personne concernée relative à l'exercice de ce droit doit être traitée « dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande »[762], sauf exception[763]. De plus, aucun paiement ne peut être exigé pour prendre toute mesure au titre du droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, à moins que la demande de la personne concernée ne s'avère manifestement infondée ou excessive[764].

---

[756] « Données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ».

[757] « La personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée ».

[758] « Le traitement est nécessaire 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 ».

[759] Art. 22, § 4, du RGPD.

[760] Voy. art. 12, §§ 2 à 6, du RGPD.

[761] Voy. chapitre 1, section 9.

[762] Art. 12, § 3, du RGPD.

[763] Pour plus de précisions sur cette question, voy. *infra*, pts 190 et 191.

[764] Art. 12, § 5, du RGPD. Pour plus de précisions sur cette question, voy. *infra*, pt 188.

SECTION 9. – Modalités de l'exercice des droits de la personne concernée (art. 12, §§ 2 à 6)

187. L'une des particularités du RGPD est qu'il régit, en son article 12, les modalités d'exercice de l'ensemble des droits de la personne concernée. Cette disposition est en effet transversale, ce qui justifie qu'une section propre lui soit consacrée.

§ 1. Facilitation de l'exercice des droits de la personne concernée

188. En vertu de cet article 12, le responsable de traitement se doit tout d'abord de faciliter l'exercice des droits conférés à la personne concernée au titre des articles 15 à 22 du RGPD[765].

Cette facilité d'exercice se traduit notamment par le fait qu'aucun paiement ne peut être demandé à la personne concernée pour la fourniture d'informations au titre des articles 13 et 14 du RGPD, ni pour procéder à toute communication et prendre toute mesure au titre des articles 15 à 22 et 34 du RGPD, à moins que les demandes de la personne concernée ne soient manifestement infondées ou excessives, notamment en raison de leur caractère répétitif[766], ce qu'il incombera au responsable de traitement de démontrer[767].

En ce cas, le responsable du traitement pourra soit refuser purement et simplement de donner suite à la demande de la personne concernée[768], soit décider de tout de même traiter cette demande, auquel cas celui-ci pourra exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, pour procéder aux communications ou pour prendre les mesures demandées[769].

§ 2. Identification de la personne concernée à l'origine de la demande

189. Le responsable de traitement se doit de vérifier l'identité de la personne concernée à l'origine de la demande, afin de s'assurer qu'il ne s'agit pas là d'une manœuvre frauduleuse d'un tiers malveillant, qui voudrait

[765] Art. 12, § 2, du RGPD.
[766] Art. 12, § 5, al. 1er, du RGPD.
[767] Art. 12, § 5, al. 2, du RGPD.
[768] Art. 12, § 5, al. 1er, b), du RGPD.
[769] Art. 12, § 5, al. 1er, a), du RGPD.

se procurer une copie des données personnelles de la personne concernée ou les effacer.

Pour ce faire, le responsable de traitement pourrait, par exemple, demander à ce que la personne concernée s'authentifie électroniquement, via une carte d'identité électronique, un *token*, un identifiant et un mot de passe, etc. Le responsable de traitement pourrait également demander à la personne concernée de lui procurer une copie de sa carte d'identité ou de tout autre document faisant foi de son identité, tel qu'un permis de conduire.

Dans la grande majorité des cas, l'identification de la personne concernée à l'origine de la demande ne posera pas problème. Si toutefois, au moment de la réception de la demande de la personne concernée, le responsable de traitement a des doutes raisonnables quant à l'identité de la personne physique présentant la demande en question, il pourra demander que lui soient fournies des informations supplémentaires nécessaires pour confirmer l'identité de cette personne concernée[770].

Notons que ce qui précède est « sans préjudice » du cas particulier de l'article 11 du RGPD, que nous avons abordé *supra*[771] et à l'analyse duquel nous nous contentons ici de renvoyer[772].

§ 3. Traitement de la demande de la personne concernée

190. Une fois la demande prise en compte, le responsable de traitement devra, dans les meilleurs délais, fournir à la personne concernée des informations sur les mesures prises à la suite de ladite demande[773]. En tout état de cause, ces informations devront être fournies dans un délai d'un mois à compter de la réception de la demande[774].

Au besoin, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes[775]. En pareil cas, le responsable de traitement devra tout de même informer la personne concernée de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande[776].

Enfin, dans l'hypothèse où le responsable de traitement déciderait ne pas donner suite à la demande formulée par la personne concernée, il devra informer celle-ci sans tarder, et au plus tard dans un délai d'un mois

[770] Art. 12, § 6, du RGPD.
[771] Voy. chapitre 1, section 1, § 2, a).
[772] Voy. *supra*, pts 27 et 28.
[773] Art. 12, § 3, du RGPD.
[774] *Ibid.*
[775] *Ibid.*
[776] *Ibid.*

à compter de la réception de la demande, des motifs de son inaction et de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle et de former un recours juridictionnel[777].

191. Le responsable de traitement devra donc, en tout état de cause, fournir des informations à la personne concernée dans un délai d'un mois à compter de la réception de la demande, que ce soit pour l'informer :

– des mesures prises à la suite de sa demande[778] ; ou
– du fait qu'il estime qu'il fait face à un cas complexe et que, par conséquent, le délai pour traiter la demande doit être prolongé de deux mois, en justifiant les motifs de cette prolongation[779] ; ou
– des motifs de son inaction et de la possibilité pour la personne concernée d'introduire une réclamation auprès d'une autorité de contrôle et de former un recours juridictionnel[780].

Dans les cas complexes, ce responsable aura au maximum trois mois à compter de la réception de la demande pour prendre attitude.

192. Enfin, signalons que les informations dont question ci-dessus doivent être, dans la mesure du possible, fournies par voie électronique à la personne concernée lorsque celle-ci a, elle-même, présenté sa demande sous une forme électronique, à moins que celle-ci n'ait demandé qu'il en soit autrement[781].

[777] Art. 12, § 4, du RGPD.
[778] Art. 12, § 3, du RGPD.
[779] *Ibid.*
[780] Art. 12, § 4, du RGPD.
[781] Art. 12, § 3, du RGPD.

CHAPITRE 2. Les limitations aux droits de la personne concernée

SECTION 1. – Une disposition transversale : l'article 23 du RGPD

193. Notre analyse des droits de la personne concernée dans le RGPD ne saurait être complète sans aborder la thématique des limitations possibles

de ces droits. À cet égard, nous avons déjà souligné, dans notre premier chapitre, que certaines limitations spécifiques à l'un ou l'autre droit de la personne concernée sont envisagées dans les dispositions mêmes du RGPD consacrant ces droits[782].

Ajoutons que le RGPD contient également, dans son chapitre IX[783], une série d'autres exceptions spécifiques aux droits de la personne concernée, que nous n'envisagerons pas dans la présente contribution, mais qu'il convient de ne pas perdre de vue[784].

194. En sus de ces limitations spécifiques, le RGPD contient une disposition transversale régissant la possible limitation de l'ensemble des droits de la personne concernée ayant été traités dans notre premier chapitre, qui est formulée comme suit :

> « Le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus aux articles 12 à 22 et à l'article 34, ainsi qu'à l'article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 à 22[785], lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir [un objectif important d'intérêt public général] »[786].

Cette disposition s'inscrit dans la filiation des deux dispositions fondamentales que sont l'article 52, paragraphe 1er, de la Charte des droits

---

[782] Art. 13, § 4, et 14, § 5 (Droit à l'information), art. 15, § 4 (Droit d'accès), art. 17, § 3 (Droit à l'effacement au sens large), art. 20, §§ 3 et 4 (Droit à la portabilité) et art. 22, §§ 2 et 3 (Droit de ne pas faire l'objet d'une décision fondée sur un traitement automatisé), du RGPD.

[783] Voy. not. l'article 85 du RGPD (Traitement et liberté d'expression et d'information), qui fait écho à l'article 9 de la Directive, ainsi que l'article 89 du RGPD (Garanties et dérogations applicables au traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques), qui fait écho à l'article 13, paragraphe 2, de la Directive.

[784] Nous invitons notamment le lecteur à se référer au Titre 17 et au Titre 19, Chapitre 3 du présent ouvrage.

[785] Cette précision était absente de la directive, qui évoquait simplement l'article 6 (équivalent de l'article 5 du RGPD) sans procéder à un tel raffinement. Il est donc patent que le RGPD, à la différence de la Directive, met l'accent sur le fait que les mesures législatives adoptées sur la base de l'article 23 du RGPD ne devraient pas permettre de limiter la substance même des principes fondamentaux relatifs aux traitements de données à caractère personnel. De fait, ces mesures peuvent uniquement engendrer des limitations aux droits que la personne concernée puise dans les exigences de cet article 5.

[786] Art. 23, § 1er, du RGPD.

fondamentaux de l'Union européenne et l'article 8, paragraphe 2, de la Convention européenne des droits de l'homme, qui ont toutes deux trait aux conditions dans lesquelles il est possible de limiter l'exercice du droit à la vie privée et à la protection des données[787]. Ce faisant, l'interprétation qui est faite de ces dispositions, respectivement par la Cour de justice de l'Union européenne et la Cour européenne des droits de l'homme, est parfaitement transposable à l'interprétation de l'article 23 du RGPD.

195. L'article 52, paragraphe 1er, de la Charte des droits fondamentaux de l'Union européenne précise ainsi que :

> « Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui »[788].

L'article 8, paragraphe 2, de la Convention européenne des droits de l'homme dispose, pour sa part, que :

> « Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui »[789].

196. À l'instar du prescrit de ces deux dispositions, il est loisible aux législateurs européens et nationaux d'adopter, en vertu de l'article 23 du RGPD, des mesures limitant les droits reconnus à la personne concernée, à la condition que celles-ci soient prévues par la loi (section 2), qu'elles respectent l'essence des libertés et des droits fondamentaux ainsi limités (section 3), qu'elles constituent une mesure nécessaire et proportionnée

[787] Art. 7 et 8 de la Charte des droits fondamentaux de l'Union européenne (2012/C 326/02), *JOUE*, C 326/391 du 26 octobre 2012 ; art. 8, § 1er, de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales signée à Rome le 4 novembre 1950.

[788] Charte des droits fondamentaux de l'Union européenne (2012/C 326/02), *JOUE*, C 326/391 du 26 octobre 2012, art. 52, § 1er.

[789] Art. 8, § 2, de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales signée à Rome le 4 novembre 1950.

dans une société démocratique (section 4) et qu'elles visent à garantir un objectif important d'intérêt public (section 5).

SECTION 2. – Mesure prévue par la loi et dispositions spécifiques minimales de l'article 23, paragraphe 2, du RGPD

197. Toute ingérence dans un droit fondamental tel que le droit à la protection des données à caractère personnel doit être prévue par une loi formulée en des termes clairs, précis et accessibles, et dont les effets sont prévisibles pour la personne concernée[790]. Il s'agit de l'exigence dite de légalité.

198. Précisons d'emblée que, en vertu de l'interprétation qui en est faite par la Cour européenne des droits de l'homme, le terme « loi » ne doit pas être compris dans son sens formel, ce qui impliquerait nécessairement l'existence d'un texte écrit ayant valeur législative, mais bien dans son acception matérielle[791] à savoir l'ensemble des règles de droit en vigueur, et non uniquement les textes de lois écrits[792].

En effet, si, à l'origine, la Cour européenne des droits de l'homme avait simplement reconnu que, dans les pays adoptant la tradition juridique de la « *Common Law* », les règles de droit non-écrites pouvaient être considérées comme satisfaisant à l'exigence de légalité de l'ingérence dans un droit fondamental[793], cette même Cour a, par la suite, reconnu aux pays s'inscrivant dans la tradition juridique du droit continental[794] une plus large marge de manœuvre quant à ce qu'il convenait d'intégrer sous le vocable de « loi »[795].

---

[790] Groupe 29, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), WP 237, 13 April 2016, p. 7.

[791] E. Degrave, *L'E-Gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, coll. du CRIDS, Bruxelles, Larcier, 2014, p. 144.

[792] R. Ergec, *Protection européenne et internationale des droits de l'homme*, 3e éd., Bruxelles, Larcier, 2014, p. 232.

[793] Cour eur. D.H., arrêt *Sunday Times c. Royaume-Uni*, 26 avril 1979, req. n° 6538/74, §§ 46 à 53.

[794] Cour eur. D.H., arrêts *Hüvig c. France*, 24 avril 1990, req. n° 11105/84, § 28 ; et *Kruslin c. France*, 24 avril 1990, req. n° 11801/85, § 29.

[795] P. De Hert, « Artikel 8. Recht op privacy », in *Handboek EVRM, Deel 2. Artikelsgewijze commentaar* (dir. J. Vande Lanotte en Y. Haeck), vol. 1, Anvers, Intersentia, 2004, p. 716.

Ainsi, la Cour a-t-elle notamment admis que les travaux parlementaires, les décisions, règlements et arrêtés de niveau inférieur à la loi, ou encore les règles de droit non-écrites, telles que les décisions jurisprudentielles, pouvaient satisfaire à l'exigence de légalité[796].

199. Outre que la limitation doive être prévue par la « loi », celle-ci doit également être formulée en de termes clairs et précis, et être suffisamment prévisible et accessible pour la personne concernée[797]. La condition d'accessibilité implique que cette dernière puisse disposer de renseignements suffisants sur les normes applicables, tandis que la condition de prévisibilité a pour conséquence que la personne concernée doit être en mesure de pouvoir prévoir, avec un degré raisonnable de certitude, les effets potentiels de cette « loi »[798].

200. Concernant cette condition particulière de la prévisibilité des effets de la « loi », il est intéressant de pointer que l'article 23 du RGPD contient un second paragraphe formulé comme suit :

> « En particulier, toute mesure législative visée au paragraphe 1 contient des dispositions spécifiques relatives, au moins, le cas échéant :
> a) aux finalités du traitement ou des catégories de traitement ;
> b) aux catégories de données à caractère personnel ;
> c) à l'étendue des limitations introduites ;
> d) aux garanties destinées à prévenir les abus ou l'accès ou le transfert illicites ;
> e) à la détermination du responsable du traitement ou des catégories de responsables du traitement ;
> f) aux durées de conservation et aux garanties applicables, en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement ;
> g) aux risques pour les droits et libertés des personnes concernées ;
> h) et au droit des personnes concernées d'être informées de la limitation, à moins que cela risque de nuire à la finalité de la limitation »[799].

Il s'agit là d'une nouveauté majeure par rapport à la Directive, qui ne contenait pas de telle disposition. Le RGPD ne laisse ainsi pas totalement

---

[796] Cour eur. D.H., arrêts *Hüvig c. France*, 24 avril 1990, req. n° 11105/84, § 28 ; et *Kruslin c. France*, 24 avril 1990, req. n° 11801/85, § 29 ; P. De Hert, « Artikel 8. Recht op privacy », *op. cit.*, p. 716.

[797] R. Ergec, *Protection européenne et internationale des droits de l'homme*, 3e éd., *op. cit.*, p. 232.

[798] *Ibid.*

[799] Art. 23, § 2, du RGPD.

carte blanche aux législateurs européens et nationaux sur cette question de la légalité de la limitation des droits de la personne concernée, dès lors que de telles mesures législatives devront nécessairement contenir, *a minima*, les dispositions spécifiques susvisées.

201. En réalité, le RGPD ne fait ici qu'intégrer les exigences de légalité et de prévisibilité qui avaient été mises en lumière par la Cour européenne des droits de l'homme dans sa jurisprudence relative à l'article 8, paragraphe 2, de la Convention européenne des droits de l'homme.

De fait, la Cour européenne des droits de l'homme a, par son illustre arrêt *Rotaru c. Roumanie*[800], défini, dès l'an 2000, les éléments devant impérativement figurer dans la « loi » limitant le droit à la vie privée, afin que celle-ci puisse être considérée comme étant suffisamment prévisible[801].

Dans cette affaire, la Cour a considéré que l'exigence de légalité n'était pas rencontrée, dès lors que la « loi » dont elle avait à connaitre :

> « ne définit ni le **genre d'informations** pouvant être consignées, ni les **catégories de personnes** susceptibles de faire l'objet des mesures de surveillance telles que la collecte et la conservation de données, ni les **circonstances** dans lesquelles peuvent être prises ces mesures, ni la **procédure** à suivre. De même, ladite loi ne fixe pas de **limite quant à l'ancienneté** des informations détenues et la **durée de leur conservation** […].
> [Cette loi] ne renferme aucune disposition explicite et détaillée sur les **personnes autorisées à consulter** les dossiers, la **nature** de ces derniers, la **procédure à suivre** et **l'usage** qui peut être donné aux informations ainsi obtenues.
> [...] bien que [ladite] loi habilite les autorités compétentes à autoriser les ingérences nécessaires afin de prévenir et contrecarrer les menaces pour la sécurité nationale, le **motif** de telles ingérences n'est pas défini avec suffisamment de précision »[802] (souligné dans le texte cité).

202. Signalons enfin que la Cour a confirmé les propos de son arrêt *Rotaru c. Roumanie*, dans son arrêt ultérieur *Shimovolos c. Russie*[803], dans lequel elle a indiqué qu'une loi encadrant la création de bases de données

---

[800] Cour eur. D.H., arrêt *Rotaru c. Roumanie*, 4 mai 2000, req. n° 28341/95.

[801] E. Degrave, *L'E-Gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, p. 163.

[802] Cour eur. D.H., arrêt *Rotaru c. Roumanie*, 4 mai 2000, req. n° 28341/95, §§ 57 et 58 ; E. Degrave, *L'E-Gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, p. 164.

[803] Cour eur. D.H., arrêt *Shimovolos c. Russie*, 21 juin 2011, req. n° 30194/09.

par des autorités publiques, contenant des données à caractère personnel de citoyens, devait nécessairement déterminer :

> « les fondements de l'enregistrement du nom d'une personne dans la base de données, les autorités compétentes pour ordonner un tel enregistrement, la durée de la mesure, la nature précise des données collectées, les procédures de stockage et d'utilisation des données collectées et les contrôles et garanties mises en place afin de prévenir les abus »[804].

SECTION 3. – Respect de l'essence des libertés et droits fondamentaux

203. Outre qu'elles doivent se conformer à l'exigence de légalité traitée ci-dessus, les mesures législatives limitant les droits de la personne concernée doivent également respecter « l'essence des libertés et droits fondamentaux »[805] de cette dernière. Ceci signifie que la mesure législative en question ne peut causer une ingérence telle qu'elle porterait atteinte à l'essence même du droit fondamental protégé, *in casu* le droit à la protection des données personnelles.

204. Cette exigence a notamment été mise en exergue par la Cour de justice de l'Union européenne dans l'affaire *Schrems*[806], dans le cadre de laquelle un citoyen autrichien, Maximillian Schrems, avait invité la Cour à se pencher sur la décision d'adéquation de la Commission européenne permettant les fluxs transfrontières de données à partir de l'Union européenne vers les entreprises américaines ayant déclaré se conformer aux principes du « *Safe Harbor* ». Ce cadre juridique était censé garantir une protection adéquate pour les traitements de données personnelles de citoyens européens qu'effectueraient ces entreprises américaines.

Or, selon Maximillian Schrems, ce « *Safe Harbor* » n'était pas suffisamment protecteur des droits des citoyens européens, dès lors qu'il était

---

[804] Cour eur. D.H., arrêt *Shimovolos c. Russie*, 21 juin 2011, req. n° 30194/09, § 69 ; E. Degrave, *L'E-Gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, *op. cit.*, p. 164. Traduction libre de : « *the grounds for registration of a person's name in the database, the authorities competent to order such registration, the duration of the measure, the precise nature of the data collected, the procedures for storing and using the collected data and the existing controls and guarantees against abuse* ».

[805] Art. 23, § 1er, du RGPD.

[806] C.J.U.E., 6 octobre 2015, *Schrems c. Data Protection Commissionner of Ireland*, affaire C-362/14.

apparu au grand jour, suite aux révélations d'Edward Snowden, que plusieurs des entreprises américaines signataires de ce « *Safe Harbor* », dont notamment Facebook, étaient contraintes de donner accès à l'ensemble des données personnelles ainsi transférées, à plusieurs services de renseignements américains, dont la National Security Agency (NSA).

Dans le cadre de cette affaire, la Cour a précisé, sur la question du respect de l'essence des libertés et des droits fondamentaux, que :

> « Une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte […].
> De même, une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte »[807].

Dans la ligne de l'analyse effectuée par la Cour de justice dans l'affaire *Schrems*, il conviendra donc d'évaluer, au cas par cas, si les mesures législatives limitant les droits de la personne concernée respectent bien l'essence même de ces droits.

SECTION 4. – Mesure nécessaire et proportionnée dans une société démocratique

205. Nous avons vu dans la section précédente que la limitation des droits de la personne concernée engendrée par la mesure législative ne pourra être disproportionnée, sous peine de porter atteinte à l'essence même de ces droits. Ceci nous permet de faire la transition avec la question de l'exigence de nécessité et de proportionnalité de la mesure législative en cause.

Ainsi, l'article 23 du RGPD précise que les États membres ne pourront adopter de mesures législatives limitant les droits de la personne concernée

[807] *Ibid.*, §§ 94 et 95.

qu'à la condition que celles-ci soient considérées comme étant nécessaires et proportionnées dans une société démocratique[808].

Conformément au prescrit de l'article 8, paragraphe 2, de la Convention européenne des droits de l'homme et de l'article 52, paragraphe 1er, de la Charte des droits fondamentaux de l'Union européenne, et à l'interprétation qui est faite de ces dispositions respectivement par la Cour de justice de l'Union européenne et la Cour européenne des droits de l'homme :

> « Toute limitation de ou interférence avec les droits fondamentaux à la vie privée et à la protection des données […] peut uniquement être justifiée si elle est "strictement nécessaire dans une société démocratique"[809] […] [ce qui implique notamment] que cette mesure doive être prise en conformité avec la loi et doive offrir "des garanties minimales contre les abus"[810] »[811].

Plus précisément, il résulte de l'analyse de la jurisprudence de la Cour européenne des droits de l'homme que celle-ci considère qu'une mesure législative ne pourra être considérée comme étant « nécessaire dans une société démocratique » que si elle se justifie pour répondre à un « besoin social impérieux »[812].

206. En outre, la Cour européenne des droits de l'homme a développé trois critères afin de déterminer si la mesure législative en cause est bien « nécessaire »[813], qui sont, selon nous, parfaitement transposable à l'article 23 du RGPD.

Le premier critère est celui de la « pertinence », à savoir qu'une mesure ne sera « nécessaire » que si elle peut être considérée comme étant utile,

---

808 Art. 23, § 1er, du RGPD.

809 Cour eur. D.H., arrêts *Klass e.a. c. Allemagne*, 6 septembre 1978, req. n° 5029/71, §§ 42 et 48 ; *Malone c. Royaume-Uni*, 2 août 1984, req. n° 8691/79, § 81 ; et *Szabo et Vissy c. Hongrie*, 12 janvier 2016, req. n° 37138/14, § 73 ; C.J.U.E., 16 décembre 2008, *Satakunnan Markkinapörssi et Satamedia*, affaire C-73/07, § 56 ; et C.J.U.E., 6 octobre 2015, *Schrems c. Data Protection Commissionner of Ireland*, affaire C-362/14, §§ 92 et 93.

810 C.J.U.E., 6 octobre 2015, *Schrems c. Data Protection Commissionner of Ireland*, affaire C-362/14, § 91 et jurisprudence citée.

811 Groupe 29, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), WP 237, 13 April 2016, p. 5.

812 R. Ergec, *Protection européenne et internationale des droits de l'homme*, 3e éd., *op. cit.*, p. 233.

813 P. De Hert, « Artikel 8. Recht op privacy », *op. cit.*, pp. 719-720.

pertinente et adéquate pour atteindre l'objectif important d'intérêt public général poursuivi[814].

Le second critère est celui de la « proportionnalité », en vertu duquel il convient de se demander s'il existe un équilibre raisonnable entre, d'une part, l'ingérence causée aux droits de la personne concernée, et, d'autre part, l'objectif important d'intérêt public général poursuivi par la mesure[815]. De fait, au plus l'objectif poursuivi s'avère être fondamental, au plus l'ingérence dans les droits de la personne concernée pourra être grande[816]. Une mesure ne pourra donc être considérée comme nécessaire que si un tel équilibre est atteint.

Le dernier critère, celui dit de « subsidiarité », a été introduit plus récemment que les deux premiers, et prévoit que l'autorité à l'origine de la mesure doit minimiser autant que faire se peut l'ingérence causée aux droits de la personne concernée, en recherchant les alternatives qui s'offrent à elle et en optant pour la mesure qui lui permettra d'atteindre l'objectif poursuivi de la manière la plus respectueuse des droits de l'homme[817]. À défaut, la mesure adoptée sans avoir effectué cette analyse risque de ne pas être qualifiée de « nécessaire ».

207. Concluons cette section en soulignant que, s'il est vrai qu'un certain nombre de critères ont été développés afin d'évaluer si la mesure législative en cause est bien nécessaire et proportionnée dans une société démocratique, il convient de ne pas perdre de vue que :

> « La Cour européenne des droits de l'homme reconnait de façon constante que les États Parties ont "une marge d'appréciation relativement large dans les choix des moyens pour atteindre le but légitime [poursuivi]"[818] lors de l'évaluation de la nécessité d'une mesure »[819].

Dans ce contexte, les législateurs européens et nationaux pourront notamment s'inspirer de la « Boîte à outils » développée par l'*European*

---

[814] Cour eur. D.H., arrêt *Handyside c. Royaume-Uni*, 7 décembre 1976, req. n° 5493/72, §§ 48-50 ; P. De Hert, « Artikel 8. Recht op privacy », *op. cit.*, p. 720.

[815] P. De Hert, « Artikel 8. Recht op privacy », *op. cit.*, p. 720.

[816] *Ibid.*

[817] Cour eur. D.H., arrêts *Hatton e.a. c. Royaume-Uni*, 8 juillet 2003, req. n° 36022/97, § 86 ; et *Peck c. Royaume-Uni*, 28 janvier 2003, req. n° 44647/98, §§ 80-87 ; P. De Hert, « Artikel 8. Recht op privacy », *op. cit.*, p. 720.

[818] Cour eur. D.H., arrêt *Weber et Saravia c. Allemagne*, 29 juin 2006, req. n° 54934/00, § 106.

[819] Groupe 29, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), WP 237, 13 April 2016, p. 5.

Data Protection Supervisor (« EDPS »), qui contient une « checklist », composée de questions spécifiques et illustrée à l'aide de décisions de jurisprudence et de cas pratiques, destinée à guider ces législateurs dans l'évaluation de la « nécessité » de la mesure qu'ils envisagent d'adopter[820].

Concrètement, cette « checklist » est composée de six étapes, à savoir (i) la description factuelle de la mesure proposée, (ii) la détermination des libertés et droits fondamentaux affectés, (iii) l'identification des objectifs poursuivis, (iv) la justification de la mesure, (v) l'effectivité de la mesure et (vi) la description des circonstances entourant la mesure[821].

SECTION 5. – Garantie d'un objectif important d'intérêt public général

208. Enfin, la limitation, par une mesure législative, des droits de la personne concernée ne sera tolérée que si cette mesure vise à garantir un des objectifs importants d'intérêt public général listés dans l'article 23 du RGPD[822].

À l'instar de ce qui était déjà contenu dans la Directive, sont ainsi évoqués :

- la sécurité nationale[823] ;
- la défense nationale[824] ;
- la sécurité publique[825] ;
- la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière[826] ;

[820] European Data Protection Supervisor, Developing a « toolkit » for assessing the necessity of measures that interfere with fundamental rights (Background paper), 16 June 2016, spéc. pp. 8-19.

[821] European Data Protection Supervisor, Developing a « toolkit » for assessing the necessity of measures that interfere with fundamental rights (Background paper), 16 June 2016, p. 9 pour le (i), pp. 10-11 pour le (ii), pp. 12-13 pour le (iii), pp. 13-14 pour le (iv), pp. 14-17 pour le (v), et pp. 17-19 pour le (vi).

[822] Art. 23, § 1er, a) à j), du RGPD.

[823] Art. 23, § 1er, a), du RGPD ; art. 13, § 1er, a), de la Directive. Notons que la Directive utilisait le vocable « sûreté de l'État ».

[824] Art. 23, § 1er, b), du RGPD ; art. 13, § 1er, b), de la Directive.

[825] Art. 23, § 1er, c), du RGPD ; art. 13, § 1er, c), de la Directive.

[826] Art. 23, § 1er, d), du RGPD ; art. 13, § 1er, d), de la Directive.

– la prévention et la détection de manquements à la déontologie des professions réglementées, ainsi que les enquêtes et les poursuites en la matière[827] ;
– une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique, dans les cas visés aux points a) à e) et g)[828] ;
– la protection de la personne concernée ou des droits et libertés d'autrui[829].

209. Le RGPD a toutefois ajouté de nouveaux objectifs importants d'intérêt public général, qui étaient absents du texte de la Directive, à savoir :

– l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces[830] ;
– la protection de l'indépendance de la justice et des procédures judiciaires[831] ;
– l'exécution des demandes de droit civil[832] ;
– **d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important** de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale[833] (nous soulignons).

210. Ce dernier objectif mérite que l'on s'y attarde quelque peu. Ainsi, s'il est vrai que la Directive faisait déjà référence à un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal[834], cet objectif a connu une transformation certaine lors de l'adoption du RGPD.

Ainsi, outre que les domaines de la santé publique et de la sécurité sociale ont été ajoutés dans le texte du RGPD, le changement majeur vient de fait que le RGPD identifie dorénavant l'intérêt économique ou financier comme étant un exemple parmi « d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre »[835].

827 Art. 23, § 1er, g), du RGPD ; art. 13, § 1er, d), de la Directive.
828 Art. 23, § 1er, h), du RGPD ; art. 13, § 1er, f), de la Directive.
829 Art. 23, § 1er, i), du RGPD ; art. 13, § 1er, g), de la Directive.
830 Art. 23, § 1er, d), du RGPD.
831 Art. 23, § 1er, f), du RGPD.
832 Art. 23, § 1er, j), du RGPD.
833 Art. 23, § 1er, e), du RGPD.
834 Art. 13, § 1er, e), de la Directive.
835 Art. 23, § 1er, e), du RGPD.

Cette modification n'est pas anodine, puisque, à la différence de l'article 13 de la Directive qui était conçu comme présentant une liste exhaustive, le RGPD contient à présent une catégorie résiduaire permettant, selon nous, aux États membres d'invoquer d'autres objectifs importants d'intérêts publics que ceux listés explicitement à l'article 23 du RGPD afin de justifier une limitation des droits de la personne concernée.

Précisons cependant que, dès lors qu'il s'agit d'une exception aux droits de la personne concernée, il conviendra d'interpréter cette disposition restrictivement, de sorte que rares devraient être les cas dans lesquels il sera acceptable de limiter ces droits pour un objectif autre que ceux listés dans cet article 23 du RGPD.

211. Quoi qu'il en soit, l'insertion d'une telle catégorie résiduaire ne manque pas de surprendre, puisque l'article 8, paragraphe 2, de la Convention européenne des droits de l'homme – que nous avons évoqué *supra*[836] et avec lequel l'article 23 du RGPD présente un lien de filiation évident – contient au contraire, et à l'instar de la Directive, une liste finie et limitative d'intérêts légitimes permettant de justifier une ingérence au droit à la vie privée[837].

Force est toutefois de reconnaitre que la formulation du texte de l'article 8, paragraphe 2, de la Convention européenne des droits de l'homme, ainsi que l'interprétation qui en est faite par la Cour européenne des droits de l'homme, sont à ce point larges que pratiquement toute mesure d'ingérence pourra être rattachée à un des intérêts légitimes[838] évoqués dans cette disposition[839].

212. Concluons cette section en précisant que, tout comme la directive 2002/58/EC[840] qu'elle vise à remplacer, la proposition de règlement du Parlement européen et du Conseil relative au respect de la vie privée et à la protection des données à caractère personnel dans les communications électroniques[841] contient également un article permettant la limitation, par

---

836 Voy. pt 195.

837 P. De Hert, « Artikel 8. Recht op privacy », *op. cit.*, p. 719.

838 À savoir : « la sécurité nationale, [la] sûreté publique, [le] bien-être économique du pays, [la] défense de l'ordre et [la] prévention des infractions pénales, [la] protection de la santé ou de la morale, ou [la] protection des droits et libertés d'autrui » (Convention de sauvegarde des droits de l'homme et des libertés fondamentales, Rome, 4 novembre 1950, art. 8, § 2).

839 P. De Hert, « Artikel 8. Recht op privacy », *op. cit.*, p. 719.

840 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, *J.O.C.E.*, 31 juillet 2002, L 201.

841 Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications

une mesure législative du droit de l'Union ou du droit des États membres, de certains droits et obligations consacrés dans cette proposition[842].

Cet article est libellé de façon semblable à l'article 23 du RGPD et procède par renvoi à cette dernière disposition pour la détermination de la liste des objectifs d'intérêt public pouvant légitimer cette limitation[843]. Notons qu'il y est fait référence à l'article 23, paragraphe 1er, e), du RGPD, de sorte que la remarque que nous avons faite ci-dessus au sujet de cette disposition nous semble pouvoir être transposée à cette proposition de règlement.

Conclusion

213. Comme indiqué en guise d'introduction au présent chapitre[844], les droits de la personne concernée, qui sont un des piliers de notre système européen de protection des données, ont subi, dans le RGPD, un lifting tantôt léger, tantôt novateur, par rapport au régime de la Directive. Au terme de notre analyse de l'ensemble de ces droits, trois conclusions transversales peuvent être dégagées.

214. Premièrement, et comme nous l'avions également indiqué dans notre introduction[845], il parait incontestable que le phénomène des réseaux sociaux a servi de toile de fond à nombre de réflexions relatives aux droits des personnes concernées, principalement pour les deux droits du RGPD qui ont fait – et feront encore – couler beaucoup d'encre, à savoir le « droit à l'oubli » et le droit à la portabilité des données.

électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »), 10 janvier 2017, COM(2017) 10 final.

842 Art. 15 de la directive 2202/58/CE et art. 11, § 1er, de cette proposition de règlement.

843 Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »), 10 janvier 2017, COM(2017) 10 final, article 11, § 1er : « Le droit de l'Union ou le droit des États membres peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus aux articles 5 à 8 lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire, appropriée et proportionnée dans une société démocratique pour préserver un ou plusieurs des intérêts publics visés à l'article 23, paragraphe 1, points a) à e), du règlement (UE) 2016/679 ou une fonction de contrôle, d'inspection ou de réglementation participant à l'exercice de l'autorité publique relativement à ces intérêts ».

844 Voy. *supra*, pt 1.

845 Voy. *supra*, pt 3.

Ainsi, le « droit à l'oubli » s'avère particulièrement pertinent pour le phénomène des réseaux sociaux, dès lors qu'il n'est pas rare que des photos ou des messages qui ont été postés plusieurs années auparavant, lorsque la personne concernée était dans un autre état d'esprit ou était simplement moins prudente, refassent surface alors que cette personne croyait ces éléments « enterrés », ce qui pourrait lui causer un préjudice. En effet, l'effacement dans le monde numérique est dépendant d'une action concrète, qui ne va pas nécessairement de soi, dès lors qu'il est plus couteux en temps, et donc financièrement, d'effacer ou d'anonymiser des données que de simplement les conserver[846].

De même, la création d'un nouveau droit à la portabilité laisse également transparaitre l'impact non-négligeable qu'a eu l'apparition des réseaux sociaux sur les réflexions de modernisation de la Directive. Cela témoigne ainsi de la volonté claire d'éviter que les personnes concernées ne soient « coincées » par les géants actuels tels que Facebook, 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.)[847].

215. Deuxièmement, nous avons pu voir, au cours de notre analyse, que les droits de la personne concernée consacrés dans le RGPD s'inscrivent dans une volonté de renforcement de l'autodétermination informationnelle de ces personnes. De fait, l'objectif de ces droits est, entre autres, de rendre aux personnes concernées une certaine forme de contrôle sur les données à caractère personnel les concernant[848], et d'assurer le respect de la dignité humaine dans un environnement toujours plus technologique.

Ainsi, ce droit à l'autodétermination informationnelle est visible en toile de fond de l'apport majeur du RGPD concernant le droit d'accès, à savoir le fait qu'il est maintenant explicitement stipulé que la personne concernée a le droit de recevoir une copie des données à caractère

[846] Voy. *supra*, pt 98.
[847] Voy. *supra*, pt 109.
[848] Le considérant n° 7 du RGPD indique à cet égard que : « Les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant ».

personnel faisant l'objet du traitement. Ceci devrait permettre de renforcer le contrôle de celle-ci sur les données personnelles la concernant[849].

Par ailleurs, le droit à l'autodétermination informationnelle est également le fondement du droit, pour la personne concernée, de recevoir des informations utiles concernant la logique sous-jacente de la décision automatisée dont elle fait l'objet[850].

Dans le même ordre d'idées, le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé vise à promouvoir l'autodétermination informationnelle et la dignité humaine. Ce droit fait, ainsi, écho à la volonté forte qu'a l'être humain de ne pas être intégralement soumis à la machine, celui-ci n'acceptant pas l'idée qu'une décision puisse lui être imposée sur la seule base de conclusions auxquelles cette machine serait parvenue, indépendamment de toute intervention humaine[851].

La volonté de mettre en place un « droit à l'oubli » est, également, ancrée dans la finalité plus large de renforcement de l'autodétermination informationnelle de la personne concernée. Ceci est d'ailleurs particulièrement pertinent au regard des spécificités de l'internet, puisque, à la différence du monde physique, l'effacement dans le monde numérique ne sera jamais automatique, et implique une action volontaire et réfléchie[852].

De même, l'un des objectifs du droit à la portabilité des données est de « rééquilibrer » la relation entre les personnes concernées et les responsables de traitements, au travers de l'affirmation des droits personnels et du contrôle des individus sur les données à caractère personnel les concernant. On voit, à nouveau, transparaitre ici la promotion du droit à l'autodétermination informationnelle[853].

Enfin, le droit pour la personne concernée de s'opposer, à tout moment et pour des raisons tenant à sa situation particulière, au profilage fondé sur l'article 6, paragraphe 1er, e) ou f), du RGPD, permet également de promouvoir le droit à l'autodétermination informationnelle de cette personne, qui désire comprendre la logique sous-jacente des traitements dont elle fait l'objet et qui la catégorisent sous tel ou tel profil[854].

216. Troisièmement, le RGPD s'attelle à offrir une protection renforcée aux enfants, compte tenu de leur plus grande vulnérabilité. En effet, le législateur européen considère que ceux-ci méritent une protection

[849] Voy. *supra*, pt 42.
[850] Voy. *supra*, pt 41.
[851] Voy. *supra*, pt 179.
[852] Voy. *supra*, pt 98.
[853] Voy. *supra*, pt 108.
[854] Voy. *supra*, pt 173.

spécifique en ce qui concerne leurs données à caractère personnel, parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel[855]. Cette protection renforcée est, en substance, assurée par deux dispositions du RGPD.

D'une part, le principe de transparence de l'article 12 du RGPD se voit renforcé lorsque les informations à fournir sont destinées spécifiquement à un enfant. En pareil cas, toute information ou communication relative à un traitement qui les concerne, devra être rédigée en des termes clairs, simples et aisément compréhensibles pour ces enfants[856].

D'autre part, l'article 17, paragraphe 1er, f), du RGPD consacre le droit de demander l'effacement des données à caractère personnel collectées dans le cadre de l'offre directe de services de la société de l'information aux enfants. Dans cette hypothèse, la personne concernée pourra, à tout moment, et sans qu'aucune justification ne doive être fournie, demander que les données en cause soit effacées, nonobstant le fait qu'elle n'est plus un enfant. Le considérant n° 65 du RGPD précise d'ailleurs que ce droit à l'effacement est particulièrement pertinent lorsque la personne concernée a donné son consentement à l'époque où elle était enfant et n'était pas pleinement consciente des risques inhérents au traitement, et qu'elle souhaite par la suite supprimer ces données à caractère personnel, en particulier sur l'internet[857].

855 Considérant n° 38 du RGPD.
856 Voy. *supra*, pt 14.
857 Voy. *supra*, pts 80 et 81.