Le consentement au traitement de données à caractère personnel à l'ère du numérique et des innovations technologiques : le crépuscule d'un mythe ?

Auteur : Beckers, Hugo
Promoteur(s) : Van Cleynenbreugel, Pieter
Faculté : Faculté de Droit, de Science Politique et de Criminologie
Diplôme : Master en droit, à finalité spécialisée en droit public et administratif (aspects belges, européens et internationaux)
Année académique : 2019-2020
URI/URL : http://hdl.handle.net/2268.2/9243

LIÈGE université
Droit, Science Politique & Criminologie

Département de Droit

TRAVAIL DE FIN D'ÉTUDES

Le consentement au traitement de données à caractère personnel à l'ère du numérique et des innovations technologiques : le crépuscule d'un mythe ?

Hugo BECKERS

Master en droit à finalité spécialisée en droit public et administratif

Année académique 2019-2020

Recherche menée sous la supervision académique de :

Monsieur Pieter VAN CLEYNENBREUGEL

Professeur de droit européen

RÉSUMÉ DU TRAVAIL

Au cœur du droit européen de la protection des données, le consentement s'est progressivement imposé comme le fondement juridique privilégié pour légitimer le traitement de données à caractère personnel. Aujourd'hui consacré à l'article 6, §1er, a), du Règlement général sur la protection des données, il représente la consécration la plus évidente du droit à l'autodétermination informationnelle, dans la droite ligne de l'article 8 de la Charte européenne des droits fondamentaux. Cependant, la place particulièrement avantageuse qui est reconnue à la manifestation de la volonté de la personne concernée est-elle toujours justifiée ?

À l'ère du numérique et des innovations technologiques, de nombreux signaux issus de la pratique révèlent l'inconsistance croissante du consentement. Sur Internet, la plupart des personnes concernées consentent machinalement au traitement de leurs données sans nécessairement prendre conscience des risques auxquels elles s'exposent. Il s'ensuit que le mythe du consentement est en réalité une protection en trompe-l'œil qui entretient l'illusion que toute personne concernée disposerait d'un contrôle absolu sur le traitement de ses données.

L'approche critique du consentement implique, tout d'abord, une analyse historique et juridique de la notion. Une fois cette première étape franchie, cette étude visera à reconsidérer la place du consentement au sein de l'édifice européen de la protection des données pour en arriver à proposer, en définitive, une solution réaliste — quoique temporaire — aux difficultés inhérentes au consentement. Cette solution passe par la recherche d'un nouvel équilibre entre les différentes bases de licéité au traitement et la consécration d'un caractère subsidiaire au consentement. La Commission européenne ainsi que le Comité européen de la protection des données pourraient entreprendre de futures démarches en ce sens. Quoi qu'il en soit, il semble que l'idée d'une érosion progressive du consentement au profit des autres bases de licéité ainsi qu'une meilleure prise en considération des évolutions technologiques devraient légitimement nourrir de nouvelles réflexions dans le domaine du droit européen de la protection des données.

REMERCIEMENTS

Parmi les personnes qui ont contribué à la réalisation de ce travail de fin d'études, j'aimerais tout d'abord remercier le Professeur VAN CLEYNENBREUGEL dont le cours de *European Law and technological innovation* a éveillé en moi l'envie de poursuivre mes recherches dans cette matière. Ses conseils, à tout stade de la préparation, m'ont par ailleurs été fort utiles.

Je tiens également à remercier Monsieur François GADISSEUR, attaché au Secrétariat général du Parlement de Wallonie et Délégué à la protection des données, pour sa disponibilité et son aide précieuse. J'ai ainsi pu compter sur son expérience pour intégrer une dimension pratique et concrète à mon travail.

Enfin, dans le contexte particulier qui nous affecte tous au moment d'écrire ces lignes, je souhaite profiter de l'occasion qui m'est donnée pour remercier ma famille, mes amis et mon entourage. À ceux-ci, je tiens à leur adresser les mots justes et vrais que Jean d'ORMESSON figea dans l'un de ses meilleurs ouvrages : « Je ne me suis pas fait avec mes propres forces. Je ne suis pas assez suffisant ni assez satisfait de moi-même pour croire que je ne dois rien aux autres. Je dois tout à ceux qui sont venus avant moi et qui m'ont instruit et élevé. Je suis le fruit d'un passé d'où je sors. Les origines me concernent comme elles vous concernent tous ».

TABLE DES MATIÈRES

INTRODUCTION

Au cœur du droit européen de la protection des données, le consentement représente la première source de licéité des opérations de traitement. Parmi les six fondements limitativement énumérés à l'article 6, §1er, du Règlement général sur la protection des données, il est le seul qui place la personne concernée au centre du dispositif légal en lui conférant la capacité d'accepter ou de refuser que ses données soient traitées à des fins déterminées. Reconnaître un véritable droit à l'autodétermination informationnelle n'est toutefois pas sans danger. C'est pourquoi le législateur européen s'est employé à renforcer les exigences de qualité du consentement en précisant que celui-ci devrait toujours être libre, spécifique, éclairé et univoque. Est-ce à dire que toute difficulté en la matière s'en trouve par conséquent écartée ? Nous ne le croyons pas. Au contraire, nous pensons que la manifestation du consentement et le respect des conditions qui l'entourent n'ont jamais autant charrié de dangers.

Pour en arriver à cette conclusion, une structure en quatre étapes est proposée. Tout d'abord, la notion du consentement sera introduite en s'appuyant sur les principaux instruments juridiques qui lui ont permis de s'enraciner progressivement dans le droit européen de la protection des données (Titre 1.). Ces premiers commentaires déboucheront sur la deuxième partie qui visera à faire la synthèse de la notion de consentement dans le cadre juridique actuellement en vigueur. Les développements théoriques seront agrémentés ça et là d'illustrations concrètes qui ne manqueront pas de révéler, dès cette étape, les difficultés pratiques inhérentes au consentement (Titre 2.). La remise en cause du consentement comme base de licéité au traitement se poursuivra au sein de la troisième étape qui évaluera le degré de protection que constitue la manifestation de la volonté à l'ère du numérique et des innovations technologiques. À cette occasion, nous constaterons que la conception traditionnelle du consentement semble de moins en moins adaptée pour répondre aux enjeux qui accompagnent l'inexorable essor des technologies du *big data* (Titre 3.). Une fois les faiblesses du consentement identifiées, nous suggérerons quelques pistes de réflexion qui permettront, selon nous, de répondre aux principaux défis auxquels le droit de la protection des données est confronté (Titre 4.).

Loin de couvrir l'intégralité de la matière, nos propos visent principalement à souligner l'inconsistance croissante du consentement manifesté dans un environnement numérique. Seuls les sujets susceptibles de nourrir les réflexions en ce sens seront donc analysés. Le consentement au traitement de données à des fins scientifiques, les transferts de données vers des pays tiers à l'Union européenne ou encore les instruments juridiques nationaux de protection des données ne feront l'objet que de commentaires ponctuels afin de réserver les principaux raisonnements à la question suivante : se dirige-t-on vers la fin du mythe du consentement ?

TITRE 1. — DE LA DIRECTIVE 95/46/CE AU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES : ÉVOLUTION DE LA NOTION DE CONSENTEMENT

1. Genèse du consentement dans le droit de l'Union européenne

Si le consentement occupe, de nos jours, une place cardinale dans le droit de la protection des données, force est de constater que cela n'a pas toujours été le cas. En effet, à l'échelle internationale, ni les lignes directrices de l'OCDE adoptées le 23 septembre 1980[1], ni les principes directeurs des Nations unies pour la règlementation des fichiers informatisés contenant des données à caractère personnel[2], ni la Convention n°108 du Conseil de l'Europe[3] n'élèvent le consentement au rang de principe de légitimation du traitement. Il en va de même au niveau national où les législations de première génération[4] ne font pas référence au consentement[5].

---

[1] Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données à caractère personnel, 23 septembre 1980 (texte disponible sur https://www.oecd.org, site consulté le 27 mars 2020). Notons que ces lignes directrices adoptées le 23 septembre 1980 ont été amendées le 11 juillet 2013 afin d'intégrer les nouvelles approches en matière de protection de la vie privée. Pour de plus amples informations sur ce document, voy. Cécile DE TERWANGNE et Jean-Marc VAN GYSEGHEM, *Vie privée et données à caractère personnel*, Bruxelles, Politeia, 2013, pp. 79 et s.

[2] Principes directeurs pour la règlementation des fichiers personnels informatisés, 14 décembre 1990 (texte disponible sur https://www.un.org, site consulté le 27 mars 2020).

[3] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 28 janvier 1981 (texte disponible sur https://www.coe.int, site consulté le 27 mars 2020). Le résumé de la Convention dispose qu'il s'agit du « premier instrument international contraignant qui a pour objet de protéger les personnes contre l'usage abusif du traitement automatisé des données à caractère personnel, et qui réglemente les flux transfrontaliers des données ».

[4] À titre d'exemple, la version d'origine de la loi belge du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel ne considérait pas le consentement comme un critère de licéité au traitement. (Sur cette loi, voy. Jos DUMORTIER et Frank ROBBEN, *Persoonsgegevens en privacybescherming, Commentaar op de wet tot bescherming van de persoonlijke levenssfeer*, Bruges, die Keure, 1995, 348 pages). Il a fallu attendre l'adoption de la loi du 11 décembre 1998 transposant la Directive 95/46/CE pour intégrer la notion de consentement en droit belge. Aux termes des travaux préparatoires, « l'article 8 du projet remplace l'actuel article 5 de la loi par un nouvel article qui reproduit l'article 7 de la directive européenne (…). La directive européenne énumère, de manière explicite et contrairement à la loi belge actuelle, les cas dans lesquels les données à caractère personnel peuvent faire l'objet d'un traitement (…). Il va de soi que le premier cas dans lequel le traitement de données à caractère personnel peut être considéré comme licite est celui auquel la personne concernée a indubitablement donné consentement » (Projet de loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil 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, *Doc.*, Ch., 1997-1998, n°1566/1, p. 31). Soulignons que la loi du 8 décembre 1992 a été abrogée et remplacée par la loi-cadre du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. Il en va de même en France où la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, plus connue sous le nom de loi informatique et libertés, ne faisait pas mention du consentement sauf en ce qui concerne les données sensibles. Elle a depuis lors profondément été remaniée et la notion de consentement y occupe désormais une place centrale. La nouvelle mouture de la loi informatique et libertés est entrée en vigueur dans une nouvelle rédaction le 1er juin 2019 afin de parachever le processus d'adaptation du droit national au RGPD (voy. Anne DEBET, Jean MASSOT et Nathalie METALLINOS, *Informatique et libertés - la protection des données à caractère personnel en droit français et européen*, Issy-les-Moulineaux, Lextenso, 2015, p. 298).

[5] Yves POULLET, « Consentement et RGPD : des zones d'ombre ! », *D.C.C.R.*, 2019/1-2, n° 122-123, p. 4.

Dans le droit de l'Union européenne, c'est à la Directive 95/46/CE 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[6] (ci-après la « Directive 95/46/CE ») que l'on doit l'introduction d'une définition du consentement[7] ainsi que la consécration de celui-ci en tant que base de licéité au traitement de données à caractère personnel[8].

Grâce à cette impulsion du Parlement européen et du Conseil, le ton était donné et les différents États membres étaient priés d'adapter leur droit interne en conséquence. Cependant, la Directive 95/46/CE n'est malheureusement pas parvenue à imposer un régime uniforme en matière de protection des données au sein de l'Union européenne notamment en raison des nombreuses fenêtres de liberté qu'elle laissait aux États membres. C'est pourquoi la Commission européenne a initié un processus de révision de la Directive 95/46/CE qui a finalement abouti à l'adoption du Règlement 2016/679 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[9] (ci-après le « RGPD »).

2. La nouvelle conception du consentement dans le RGPD

Parmi les sujets abordés au cours des discussions préalables à l'adoption du RGPD, il convenait de redéfinir le consentement et de fixer la place qu'il allait occuper dans le nouveau texte. Bien loin d'abandonner la notion de consentement, le législateur européen a au contraire décidé de la placer au centre de l'édifice de protection des données[10]. Ainsi, selon le Parlement européen, « le consentement devrait demeurer l'élément clé de l'approche de la protection des données de l'Union européenne, puisqu'il s'agit du meilleur moyen pour que les personnes puissent contrôler les activités de traitement des données »[11]. À cet égard, de nombreux auteurs

---

[6] 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.*, L 281 du 23 novembre 1995, pp. 31-50. Sur cette directive, voy. Marie-Hélène BOULANGER, Cécile DE TERWANGNE, Thierry LEONARD, Sophie LOUVEAUX, Damien MOREAU et Yves POULLET, « La protection des données à caractère personnel en droit communautaire », *J.T. dr. eur.*, 1997, pp. 121 et s.

[7] « Consentement de la personne concernée : toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement » (article 2, h), de la Directive 95/46/CE).

[8] « Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si: a) la personne concernée a indubitablement donné son consentement » (article 7, a), de la Directive 95/46/CE).

[9] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L 119 du 4 mai 2016, pp. 1-88.

[10] Cécile DE TERWANGNE et Karen ROSIER, *Le règlement général sur la protection des données (RGPD/GDPR) - Analyse approfondie*, Bruxelles, Larcier, 2018, p. 121.

[11] Comité LIBE du Parlement européen du 22 novembre 2013 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) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Rapporteur Jan Philipp ALBRECHT, Exposé des motifs, pp. 218-219.

voient à travers le consentement, la parfaite consécration du *Privacy self-management* qui fonde le droit de tout individu à disposer librement de ses propres données[12].

Dans le monde numérique qui ne cesse de se complexifier, un consentement non-balisé représente cependant un réel danger[13]. Ce constat correspond à la situation qui prévalait lorsque la Directive 95/46/CE était encore en vigueur. En effet, le recours au consentement pour justifier le traitement de données à caractère personnel était de loin la base légale la plus répandue. Certains responsables du traitement n'avaient parfois aucun scrupule à exploiter les données personnelles des individus après avoir recueilli de ceux-ci un consentement de mauvaise qualité[14]. Les autres fondements de licéité du traitement tels que la poursuite d'un intérêt légitime ou l'exécution d'un contrat étaient, à l'inverse, délaissés.

Conscient des dérives qui se multipliaient sous le couvert d'un consentement basé sur le silence, le législateur européen s'est employé à fixer de nouvelles exigences de qualité au sein du RGPD. Ainsi, au-delà des caractéristiques qu'il présentait déjà sous la Directive 95/46/CE, à savoir être libre, spécifique et éclairé[15], le consentement doit désormais être univoque, c'est à dire manifesté par un acte positif clair. Il n'est donc plus permis de légitimer un traitement sur la base d'un consentement par défaut. Autre nouveauté, le responsable du traitement est à présent tenu de prouver l'existence et la qualité du consentement qu'il reçoit de la personne concernée par le traitement. Le RGPD précise également que le consentement est révocable et qu'il doit être aussi simple de le retirer que de le donner[16].

Bien que la nouvelle conception du consentement ait nettement amélioré la situation, nous pensons comme d'autres[17] que ces précautions ne suffisent pas à garantir un consentement qui corresponde à la véritable expression de l'autonomie du sujet. Lorsque la personne concernée est invitée à donner son consentement, elle ne mesure pas toujours la portée de son choix. Dans un environnement numérique en constant développement, il est hélas de plus en plus probable que les consentements creux et mécaniques deviennent monnaie courante. C'est ce qui nous

---

[12] Voy. notamment Yves POULLET, *La vie privée à l'heure de la société du numérique*, Bruxelles, Larcier, 2019, p. 126 ; Marcin BETKIER, *Privacy Online, Law and the Effective Regulation of Online Services,* Cambridge, Intersentia, 2019, pp. 33 et s. ; Bart Willem SCHERMER, Bart CUSTERS et Simone VAN DER HOF, « The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection », *Ethics & Information Technology*, 2014/16, p. 174 et Eleni KOSTA, *Consent in European Data Protection Law,* Leiden, Martinus Nijhoff, 2013, p. 140.

[13] Daniel SOLOVE, « Introduction : Privacy Self-Management and the Consent Dilemma », *Harvard Law Review*, 2013/126, p. 1880 et Julie COHEN, « Between Truth and Power », *in* Mireille HILDEBRANDT et Bibi VAN DEN BERG (eds.), *Information, Freedom and Property,* Routledge, Abingdon, 2016, pp. 68-69.

[14] Benjamin DOCQUIR, *Répertoire pratique du droit belge - Législation, Doctrine, Jurisprudence - Droit du numérique,* Bruxelles, Larcier, 2018, p. 427 et Cécile DE TERWANGNE et Karen ROSIER, *op. cit.*, p. 121.

[15] Notons que la Directive 95/46/CE utilisait le terme « informé » alors que le RGPD exige dorénavant que le consentement soit « éclairé ». La version anglaise du RGPD n'a pas connu cette adaptation de sorte qu'elle utilise encore la notion d'*« informed consent »*. Nous croyons par conséquent, que cette évolution terminologique dans la version française du RGPD ne représente aucune évolution sur le fond.

[16] Yves POULLET, *La vie privée à l'heure de la société du numérique*, *op. cit.*, pp. 127-128.

[17] Voy. notamment Yves POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.,* p. 10.

porte à croire que le consentement n'a jamais cessé d'évoluer et qu'au cours des prochaines années, il ne manquera pas de poursuivre sa mue vers de nouvelles formes.

3. L'article 8 de la Charte européenne des droits fondamentaux comme consécration du droit à l'autodétermination informationnelle

Depuis l'entrée en vigueur du Traité de Lisbonne, la Charte européenne des droits fondamentaux du 7 décembre 2000 est devenue juridiquement contraignante. L'article 6 du Traité sur l'Union européenne dispose à ce titre que « l'Union reconnaît les droits, les libertés et les principes énoncés dans la Charte des droits fondamentaux de l'Union européenne (…) laquelle a la même valeur juridique que les traités. Les dispositions de la Charte n'étendent en aucune manière les compétences de l'Union telles que définies dans les traités »[18].

Parmi les libertés fondamentales qu'elle défend, outre la protection de la vie privée, la Charte est le premier texte d'une portée générale qui consacre une disposition spécifique à la protection des données[19]. L'article 8 de la Charte énonce que « toute personne a droit à la protection des données à caractère personnel la concernant. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification »[20]. L'article 16 du Traité sur le fonctionnement de l'Union européenne reproduit le libellé de l'article 8 de la Charte. Il fonde par ailleurs la compétence du Parlement européen et du Conseil pour adopter les règles nécessaires à la protection des données à caractère personnel au sein de l'Union[21].

L'article 8 de la Charte ne se résume pas à garantir, d'une manière générale, un droit à la protection des données. En effet, il précise que lorsque le traitement de données à caractère personnel est envisagé, celui-ci doit être réalisé dans le respect du principe de loyauté. De plus, les données collectées doivent pouvoir être consultées par la personne concernée et, le cas échéant, il faut pouvoir en obtenir la rectification[22]. Soulignons enfin que tout traitement doit être effectué en vertu d'un fondement juridique spécialement envisagé dans une loi. La mention explicite du seul consentement comme source de licéité au traitement n'est pas anodine. Elle révèle l'intention des auteurs de la Charte de faire du consentement le pilier

---

[18] Article 6 du Traité sur l'Union européenne (texte disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:12012P/TXT, site consulté le 29 mars 2020).

[19] Anne DEBET, Jean MASSOT et Nathalie METALLINOS, *op. cit.,* p. 74 et Jean-Marc VAN GYSEGHEM, Cécile DE TERWANGNE, Jean HERVEG et Claire GAYREL, « La protection des données à caractère personnel en droit européen - Data Protection in European Law », *JEDH*, 2014/1, pp. 60-61.

[20] Article 8 de la Charte européenne des droits fondamentaux du 7 décembre 2000 (texte disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:12012P/TXT, site consulté le 29 mars 2020).

[21] Yves POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.,* p. 5.

[22] Anne DEBET, Jean MASSOT et Nathalie METALLINOS, *op. cit.,* pp. 74-75.

essentiel de la protection des données[23]. Au cœur des droits fondamentaux de l'Union, le consentement apparaît comme le symbole le plus évident du droit à l'autodétermination informationnelle pour tout traitement de données à caractère personnel.

[23] Yves POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.,* p. 4 et Christopher KUNER, *European Data Privacy Law and Online Business,* Oxford, Oxford University Press, 2003, pp. 16-17.

TITRE 2. — LE CONSENTEMENT AU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL : ANALYSE DES TEXTES

1. Aperçu des différentes hypothèses de licéité au traitement

Dans le droit de l'Union européenne, le traitement de données à caractère personnel « n'est licite que si, et dans la mesure où »[24] il se fonde sur une cause de licéité répertoriée à l'article 6 du RGPD[25]. En d'autres termes, cette approche, qui fait écho à l'article 8 de la Charte européenne des droits fondamentaux, interdit de manière générale tout traitement à moins que celui-ci ne rencontre précisément l'une des hypothèses dans laquelle il est autorisé[26]. Dans un important arrêt, la Cour de justice a reconnu le caractère exhaustif et limitatif de différentes causes de licéité de sorte que « les États membres ne sauraient ni ajouter de nouveaux principes relatifs à la légitimation des traitements de données à caractère personnel à l'article 7 de la Directive 95/46/CE ni prévoir des exigences supplémentaires qui viendraient modifier la portée de l'un des six principes prévus à cet article »[27]. Malgré les nombreuses adaptations et précisions apportées par le RGPD, les six hypothèses de licéité qu'il énonce correspondent globalement à celles déjà admises par la Directive 95/46/CE. L'enseignement de la Cour conserve dès lors toute sa pertinence dans le cadre de l'analyse de l'actuel article 6 du RGPD.

Le consentement occupe symboliquement la tête de l'énumération de l'article 6 du RGPD. Même si aucune hiérarchie n'est instituée entre les fondements[28], la place avantageuse du consentement témoigne de son importance dans le droit de la protection des données. Sont ensuite successivement justifiés les traitements nécessaires à l'exécution d'un contrat, au respect d'une obligation légale, à la sauvegarde d'intérêts vitaux, à l'exécution d'une mission d'intérêt public ou aux fins d'intérêts légitimes poursuivis par le responsable du traitement[29].

Bien que juridiquement équivalents, les six fondements ne sont pas équitablement utilisés dans la pratique. En effet, force est de constater que le consentement demeure la voie privilégiée par

---

[24] Article 6, §1er, du Règlement général sur la protection des données (RGPD).

[25] Au-delà de l'exigence de fonder tout traitement sur l'une des hypothèses visées à l'article 6 du RGPD, le principe de licéité consacré à l'article 5, §1er, du RGPD signifie que l'ensemble des règles légales applicables doivent être respectées par le responsable du traitement. Il s'ensuit que pour être licite au sens large, un traitement doit non seulement respecter les règles en matière de protection des données mais aussi, par exemple, les obligations en matière de droit du travail ou de protection des consommateurs. (Voy. Cécile DE TERWANGNE, Elise DEGRAVE, Antoine DELFORGE, et Loïck GÉRARD, *La protection des données à caractère personnel en Belgique*, Bruxelles, Politeia, 2019, p. 33).

[26] Olivia TAMBOU, *Manuel de droit européen de la protection des données à caractère personnel*, Bruxelles, Bruylant, 2020, pp. 114-115 et Cécile DE TERWANGNE et Karen ROSIER, *op. cit.*, pp. 118-119.

[27] C.J.U.E., 24 novembre 2011, *arrêt ASNEF et FECEMD c. Administracion del Estado*, C-468/10 et C-469/10, pt. 32.

[28] Jean-Ferdinand PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : *in causa venenum ?* », *DCCR,* 2019/122-123, p. 47.

[29] Article 6, §1er, a) à f) du Règlement général sur la protection des données (RGPD).

la plupart des responsables du traitement[30] pour exploiter les données des personnes concernées[31]. Si certains s'en réjouissent[32], d'autres ne font pas preuve du même enthousiasme et émettent quelques réserves[33]. Notre propos — et nous y reviendrons *infra* — consistera à conserver le consentement comme source de licéité au traitement tout en lui reconnaissant un caractère subsidiaire. Selon nous, cette approche, à contre-courant de la tendance majoritaire, permettrait d'atteindre le délicat équilibre entre le droit à l'autodétermination des personnes concernées par un traitement de données et le devoir des autorités publiques de garantir leur protection.

2. Un consentement de qualité comme fondement de licéité au traitement

On l'a vu, tout traitement de données à caractère personnel doit se fonder sur une des bases légales énumérées à l'article 6 du RGPD. Parmi celles-ci, le consentement qui occupe la première place, matérialise un véritable droit à l'autodétermination informationnelle des personnes concernées sur leurs données. L'article 4, 11° du RGPD définit le consentement comme « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ». Chacun des qualificatifs mérite des commentaires approfondis. Ainsi, les exigences d'un consentement libre (2.1.), spécifique (2.2.), éclairé (2.3.) et univoque (2.4.) seront successivement abordées. Des exemples concrets permettront également de mieux en cerner les contours.

2.1. Un consentement libre

Alors que la Directive 95/46/CE se contentait d'évoquer de manière évasive le caractère libre que doit présenter un consentement de qualité, le RGPD est, à cet égard, nettement plus précis. La manifestation d'une volonté libre sera d'abord envisagée de manière générale (2.1.1) avant d'en définir les limites à travers une série de circonstances concrètes où le responsable du traitement jouit d'une place dominante par rapport à la personne concernée par un éventuel traitement de ses données (2.1.2).

---

[30] L'expression d'un consentement pour fonder le traitement de données est la voie qu'empruntent de nombreux responsables du traitement dans le secteur privé. En revanche, cette base de licéité reste plutôt rare dans le secteur public où les responsables du traitement justifient principalement leurs opérations sur la base d'une obligation légale qu'ils se doivent de respecter (article 6, §1er, c), du RGPD) ou lorsqu'elles sont nécessaires à l'exécution d'une mission d'intérêt public (article 6, §1er, e), du RGPD). (Informations recueillies le 7 avril 2020 auprès de Monsieur François GADISSEUR, délégué à la protection des données au sein du Parlement de Wallonie).

[31] L'une des raisons qui explique sans aucun doute le succès que rencontre le consentement par rapport aux autres fondements de licéité est inscrit à l'article 6, §4 du RGPD. On y découvre ainsi qu'en cas de changement de finalités, le responsable du traitement est tenu de vérifier si le nouveau traitement est compatible avec les finalités pour lesquelles les données à caractère personnel ont été initialement collectées *sauf* si le traitement antérieur se fondait sur le consentement de la personne concernée.

[32] Voy. notamment Jean-Ferdinand PUYRAIMOND, *op. cit.*, pp. 46-47.

[33] Voy. notamment Yves POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.,* p. 20.

2.1.1. Manifestation de volonté libre

Comme l'indique le considérant 42 du RGPD, pour qu'un consentement soit considéré comme ayant été librement donné, la personne concernée par un traitement de données doit disposer d'une véritable liberté de choix. Elle doit ainsi être en mesure de refuser ou de retirer son consentement sans subir de préjudice, sous quelque forme que ce soit. La notion de préjudice est interprétée largement de sorte que la tromperie, l'intimidation, la coercition ou toute autre conséquence négative représentent des entraves à un consentement libre[34]. Aucune pression, même purement commerciale[35], ne peut orienter la personne concernée à choisir entre donner ou ne pas donner son consentement. Le cas échéant, la charge de la preuve du caractère libre du consentement repose sur le responsable du traitement[36].

La question s'est également posée de savoir si la fourniture d'un service peut ou non être conditionnée à l'obtention d'un consentement. En d'autres termes, le service dont l'utilisation serait subordonnée à la délivrance d'un consentement représente-t-il un obstacle au caractère libre du consentement dès lors que rien n'oblige la personne concernée à utiliser le service visé ?

Il ressort de l'article 7, §4, du RGPD que le consentement est présumé ne pas avoir été donné librement lorsque l'exécution d'un contrat, y compris la prestation d'un service, est subordonnée au consentement au traitement de données alors que ce traitement n'est pas strictement nécessaire à l'exécution dudit contrat[37]. Par conséquent, la prestation d'un service ne devrait pas être conditionnée au consentement de la personne concernée par un traitement qui poursuit des finalités qui ne sont pas nécessaires à la prestation du service[38]. Par cette disposition, le législateur européen veille à éviter que l'obtention d'un consentement rende légitime les traitements parasites de données[39]. Il est donc fortement déconseillé aux responsables du traitement de chercher à obtenir l'accord de la personne concernée pour

---

[34] Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679,* 17/FR WP 259, révisées et adoptées le 10 avril 2018, p. 12. Document disponible sur https://www.cnil.fr/sites/default/files/atoms/files/ldconsentement_wp259_rev_0.1_fr.pdf, site consulté le 31 mars 2020.

[35] Il faut entendre par pression commerciale, les frais et coûts supplémentaires qui résulteraient du refus ou du retrait du consentement. (Voy. Yves POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.,* p. 6).

[36] Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679, op. cit.,* p. 12.

[37] La locution « nécessaire à l'exécution d'un contrat » doit être interprétée de manière restrictive. (Voy. Groupe de travail de l'article 29, *Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE,* 844/14/FR WP 217, adopté le 9 avril 2014, pp. 18-19. Document disponible sur https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf, site consulté le 31 mars 2020).

[38] Benjamin DOCQUIR, *Vers un droit européen de la protection des données ?*, Bruxelles, Larcier, 2017, p. 95.

[39] Axel BEELEN, *Guide pratique du RGPD - Fiches de guidance,* Bruxelles, Bruylant, 2018, p. 45.

exploiter ses données conformément à des finalités qui sortent du champ d'application du contrat en cause[40].

On soulignera, par ailleurs, que la présomption de l'article 7, §4, du RGPD ne s'applique qu'aux cas où les données réclamées ne sont pas nécessaires à l'exécution d'un contrat ou à la fourniture d'un service. Comme le note le Groupe de travail de l'article 29[41] dans ses *Guidelines*, « si le traitement est nécessaire à l'exécution d'un contrat (y compris à la fourniture d'un service), l'article 7, paragraphe 4 ne s'applique pas »[42]. En effet, si le responsable du traitement souhaite traiter des données qui se révèlent être nécessaires à l'exécution d'un contrat, le consentement n'est pas la base juridique la plus appropriée pour légitimer le traitement.

2.1.2. Validité du consentement dans le contexte particulier d'un *« imbalance of powers »*

Dans le prolongement des développements qui précèdent, il convient d'être particulièrement attentif aux situations dans lesquelles un déséquilibre de pouvoirs manifeste caractérise la relation entre le responsable du traitement et la personne concernée. Le considérant 43 du RGPD, qui vise spécialement cette difficulté précise qu'afin de « garantir que le consentement [soit] donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel dans un cas particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement (…) et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière »[43]. L'hypothèse d' *« imbalance of powers »* entre les acteurs d'un traitement sera successivement abordée dans le cadre des relations de travail (2.1.2.1), des relations avec une autorité publique (2.1.2.2) ainsi que dans les situations particulières de monopoles (2.1.2.3).

2.1.2.1. Relations de travail

La première hypothèse dans laquelle un déséquilibre manifeste peut se marquer entre les parties à un traitement de données est rencontrée dans le domaine des relations de travail. En

---

[40] Par exemple, l'entreprise spécialisée dans la vente de vêtements en ligne peut raisonnablement attendre de son client qu'il consente à lui transmettre son adresse pour mener à bien la livraison des achats. Elle ne peut en revanche pas conditionner la livraison des vêtements à l'obtention d'un consentement qui permettrait la collecte des données personnelles de l'acheteur à des fins de publicité comportementale. En effet, dans ce cas, le consentement serait considéré comme n'ayant pas été librement donné.

[41] Ce groupe de travail était un organe consultatif européen indépendant qui a été institué par l'article 29 de la Directive 95/46/CE. Il traitait les questions relatives à la protection de la vie privée et aux données à caractère personnel jusqu'au 25 mai 2018, date à laquelle le RGPD est devenu applicable. L'organe qui remplace le Groupe de l'article 29 est le Comité européen de la protection des données (CEPD).

[42] Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679, op. cit.,* p. 10.

[43] Considérant 43 du Règlement général sur la protection des données (RGPD).

effet, compte tenu du rapport de subordination d'un employé à l'égard de son employeur, il est peu probable que l'employé ne ressente aucune pression — fût-elle uniquement implicite — s'il venait à s'opposer au traitement de ses données. Il s'ensuit que l'employeur qui souhaite exploiter les données de ses employés aurait tout intérêt à fonder son traitement sur une autre base juridique que le consentement[44].

Le législateur européen est conscient des difficultés qui résultent des relations de travail dans le cadre du droit de la protection des données. Il ne fournit cependant aucune réponse claire à ce sujet[45]. Il renvoie au contraire au droit des États membres, en permettant à ceux-ci de prévoir, par la loi ou au moyen de conventions collectives, des règles plus spécifiques pour assurer la protection des droits et libertés des employés dans le cadre des relations de travail[46].

2.1.2.2.Relations avec une autorité publique

L'équilibre des rapports de force nécessaire à la manifestation d'une volonté libre est également remise en cause lorsqu'une autorité publique entre en relation avec un administré. Outre la place privilégiée dont bénéficie une administration, il est clair que l'administré concerné par le traitement de ses données n'aura pas d'autre solution réaliste que celle de consentir au traitement[47]. Cette règle n'est toutefois pas absolue de sorte qu'une administration peut valablement recourir au consentement comme base de licéité au traitement dans certaines circonstances particulières[48].

2.1.2.3.Monopoles et biens de première nécessité

Il existe enfin une dernière hypothèse dans laquelle le déséquilibre des rapports de force ne s'explique pas en raison de la qualité des parties mais bien de la nature d'une relation ou du type de bien faisant l'objet d'une transaction. Nous croyons en effet que le responsable du traitement qui profite d'une situation monopolistique exerce, par la force des choses, une pression quasiment insurmontable sur la personne concernée dès lors que cette dernière est

---

[44] Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679, op. cit.,* pp. 7-8.

[45] Benjamin DOCQUIR, *Répertoire pratique du droit belge - Législation, Doctrine, Jurisprudence - Droit du numérique, op. cit.*, pp. 435-436.

[46] Voy. l'article 88 du Règlement général sur la protection des données (RGPD).

[47] Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679, op. cit.,* pp. 6-7.

[48] Par exemple, c'est le cas lorsqu'une personne est invitée à cocher une case pour consentir au traitement de ses données à caractère personnel dans la cadre du dépôt et de la signature d'une pétition en ligne sur le site Internet d'une assemblée législative. Ainsi, pour déposer et signer une pétition par voie électronique sur le site web du Parlement de Wallonie, il est nécessaire d'accepter que son nom et son prénom soient repris sur le site web du Parlement ainsi qu'au Bulletin des pétitions. Les données personnelles du pétitionnaire sont également transmises aux députés qui examinent la pétition. Ici, il est clair que la demande de consentement ne s'accompagne d'aucune pression de sorte que la personne concernée reste totalement libre de consentir ou non au traitement de ses données. (Informations recueillies le 7 avril 2020 auprès de Monsieur François GADISSEUR, délégué à la protection des données au sein du Parlement de Wallonie).

dans l'incapacité matérielle de disposer d'un bien ou d'un service équivalent auprès d'une entité concurrente. Notons que plus un bien ou un service est entré dans les mœurs, plus la pression qui s'exerce sur la personne concernée au moment de consentir ou non au traitement de ses données est grande.

Un raisonnement analogue peut selon nous s'appliquer aux biens de première nécessité. Compte tenu de la dépendance de la personne concernée aux biens en question, il n'est pas déraisonnable d'envisager que le responsable du traitement qui administre la distribution desdits biens profite de sa situation privilégiée pour obtenir un consentement forcé au traitement de données.

2.2. Un consentement spécifique

Lorsqu'un traitement de données poursuit plusieurs finalités spécifiques, la personne concernée doit pouvoir marquer son consentement pour chacune de ces finalités[49]. Le consentement n'est donc pas un blanc seing qui permettrait au responsable du traitement de faire ce qu'il veut des données collectées[50]. Le considérant 32 du RGPD précise en ce sens que « le consentement donné devrait valoir pour toutes les activités de traitement ayant la ou les mêmes finalités. Lorsque le traitement a plusieurs finalités, le consentement devrait être donné pour l'ensemble d'entre elles »[51]. Cette exigence, dite de « granularité », vise à garantir un degré élevé de transparence pour que la personne concernée agisse en pleine connaissance de cause[52].

Par ailleurs, il convient de souligner qu'aux termes de l'article 7, §2, du RGPD, « si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions »[53]. Cette disposition est étroitement liée au caractère éclairé que doit présenter le consentement. En effet, la séparation nette qui est ainsi exigée pour la présentation de la demande de consentement veille à renforcer l'information de la personne concernée qui s'apprête à consentir au traitement de ses données[54].

---

[49] Concrètement, le caractère spécifique du consentement implique que la personne concernée doit, si elle le souhaite, pouvoir consentir à certaines finalités et pas à d'autres. Combinée à l'exigence d'un consentement libre, cette « granularité » du consentement ne doit pas exposer la personne concernée à un préjudice si elle décide de ne pas consentir à toutes les finalités qui lui sont présentées.

[50] Cécile DE TERWANGNE et Karen ROSIER, *op. cit.*, p. 123 et Benjamin DOCQUIR, *Répertoire pratique du droit belge - Législation, Doctrine, Jurisprudence - Droit du numérique, op. cit.*, pp. 431-432.

[51] Considérant 32 du Règlement général sur la protection des données (RGPD).

[52] Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679, op. cit.,* p. 13.

[53] Article 7, §2, du Règlement général sur la protection des données (RGPD).

[54] Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679, op. cit.,* pp. 13-14.

2.3. Un consentement éclairé

Pour qu'un consentement soit considéré comme éclairé, il est essentiel que la personne concernée ait été avertie de certains éléments cruciaux avant de manifester sa volonté. Le considérant 42 du RGPD recommande en ce sens que la personne concernée devrait « connaître au moins l'identité du responsable du traitement et les finalités du traitement auquel sont destinées ses données à caractère personnel »[55]. Le Groupe de travail de l'article 29 ajoute une série d'exigences minimales qui doivent être communiquées par le responsable du traitement à la personne concernée. Il s'agit, d'apporter des informations sur les types de données collectées, sur l'existence du droit de retirer son consentement[56], sur l'utilisation éventuelle de données pour une prise de décision automatisée[57] ainsi que sur les risques potentiels liés à la transmission des données vers un pays n'offrant pas des garanties appropriées telles que décrites à l'article 46 du RGPD[58]. Une fois transmises, ces informations devraient permettre à la personne concernée de comprendre ce à quoi elle s'engage en toute connaissance de cause[59].

Naturellement, il ne faut pas que la forme sous laquelle les informations sont communiquées rende ces dernières inintelligibles. Ainsi, le responsable du traitement doit constamment veiller à employer des termes clairs, compréhensibles et accessibles. Le vocabulaire trop technique et les notices absconses sont donc à éviter[60]. En toute hypothèse, le responsable du traitement doit identifier le public cible et adapter la forme des informations transmises en conséquence. Si les personnes concernées sont mineures[61], le responsable du traitement est tenu de faire preuve d'un surcroît de pédagogie[62].

---

[55] Considérant 42 du Règlement général sur la protection des données (RGPD).

[56] Voy. l'article 7, §3, du Règlement général sur la protection des données (RGPD).

[57] Voy. l'article 22, §2, c), du Règlement général sur la protection des données (RGPD). Pour de plus amples détails, nous renvoyons aux lignes directrices du Groupe de travail de l'article 29 sur *les décisions individuelles automatisées et le profilage au titre du Règlement 2016/679,* 17/EN WP 251, révisées et adoptées le 6 février 2018, pp. 20 et s. Document disponible sur https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, site consulté le 1er avril 2020.

[58] Voy. l'article 49, §1er, a), du RGPD.

[59] Cécile DE TERWANGNE et Karen ROSIER, *op. cit.*, pp. 124-125 et Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679, op. cit.,* p. 15.

[60] Benjamin DOCQUIR, « Consentement et intérêt légitime dans le secteur privé », *in* Nathalie RAGHENO (coord.), *Data Protection & Privacy. Le GDPR dans la pratique/De GDPR in de praktijk,* Limal, Anthemis, 2017, p. 33.

[61] Sur le principe de transparence qui est indispensable lorsque des informations sont communiquées au public et en particulier aux enfants, nous renvoyons au considérant 58 du RGPD.

[62] Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679, op. cit.,* p. 16.

2.4. Un consentement univoque

Un consentement de qualité suppose que le choix de la personne concernée soit clair et certain. Ce consentement qui peut être explicite ou implicite (2.4.1.) doit être manifesté par une déclaration ou un geste actif (2.4.2.).

2.4.1. Un consentement explicite ou implicite

Sous l'empire de la Directive 95/46/CE, le consentement devait être indubitable pour permettre le traitement de données ordinaires et explicite pour tout traitement se rapportant à des données sensibles. Au cours des discussions préalables à l'adoption du RGPD, le Parlement et la Commission suggérèrent de renforcer la protection des personnes concernées en généralisant l'exigence d'un consentement explicite pour légitimer le traitement de tout type de données. Cette intention visait à lutter contre la multiplication des consentements de mauvaise qualité perçus sur Internet, au moyen d'outils numériques en perpétuel développement[63]. Cependant, le Conseil a préféré retenir l'exigence d'un consentement univoque pour légitimer les traitements de données non-sensibles[64].

Pour qu'un consentement soit qualifié d'univoque, le responsable du traitement doit s'assurer que la personne concernée a délibérément donné son approbation au traitement. En d'autres termes, le consentement ne peut ni être présumé ni résulter du silence ou de l'inactivité de la personne concernée[65]. Ainsi, le recours à des cases pré-cochées[66], les options de refus non-complétées, les conditions générales réputées acceptées[67], la simple poursuite de l'utilisation

---

[63] Cécile DE TERWANGNE et Karen ROSIER, *op. cit.*, p. 125.

[64] L'essor des technologies du numérique s'accompagne de multiples mises en garde issues de la pratique et ensuite relayées dans la doctrine. En ce qui concerne le cas particulier du consentement, le Groupe de travail de l'article 29 note que de nombreux utilisateurs « reçoivent chaque jour de nombreuses demandes de consentement auxquelles [ils] doivent répondre par un clic ou en balayant leur écran. Cela peut mener à une certaine lassitude: lorsque trop souvent rencontré, l'effet d'avertissement des mécanismes de consentement diminue. Il en résulte une situation où les informations de consentement cessent d'être lues. Cela constitue un grand risque pour les personnes concernées, dès lors que le consentement est généralement demandé pour des actions qui seraient illicites sans ce consentement » (Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679, op. cit.,* p. 20). En dépit de ces avertissements, le Conseil a adopté une attitude timorée en refusant de suivre l'option dégagée par le Parlement et la Commission, ce que nous regrettons. Nous pensons en effet qu'une généralisation du caractère explicite du consentement aurait significativement renforcé la protection des personnes concernées par le traitement de leurs données sans pour autant fragiliser excessivement le consentement en tant que base de licéité au traitement.

[65] Benjamin DOCQUIR, *Répertoire pratique du droit belge - Législation, Doctrine, Jurisprudence - Droit du numérique, op. cit.*, p. 428.

[66] Ce procédé est spécialement visé au sein du considérant 32 du RGPD qui dispose qu'il « ne saurait y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité » (considérant 32 du Règlement général sur la protection des données (RGPD).

[67] Benjamin DOCQUIR, *Répertoire pratique du droit belge - Législation, Doctrine, Jurisprudence - Droit du numérique, op. cit.*, p. 429.

ordinaire d'un site Internet[68] ou toute autre forme de consentement par défaut[69] ne peuvent en aucun cas justifier le traitement de données personnelles.

Si l'exigence d'univocité n'admet pas qu'un consentement puisse reposer sur l'inaction de la personne concernée, elle ne s'oppose pas à ce que la volonté de l'intéressé soit extériorisée de manière implicite. Le caractère implicite du consentement doit être interprété strictement de sorte que les circonstances ne doivent souffrir d'aucune ambiguïté quant à l'existence du consentement[70].

Signalons enfin que le RGPD prévoit une série d'hypothèses dans lesquelles seul un consentement explicite est admis. Cette protection renforcée veille à garantir à la personne concernée un niveau élevé de contrôle sur certaines de ses données sensibles. Les traitements qui nécessitent un consentement explicite sont ceux qui portent sur les catégories particulières de données énumérées à l'article 9 du RGPD, impliquent un flux transfrontière en dehors de l'Union, ou prévoient une exploitation automatisée des données[71].

2.4.2. Manifestation du consentement par une déclaration ou un acte positif clair

La meilleure façon d'établir que la personne concernée consent au traitement de ses données consiste à exiger d'elle une déclaration ou un acte positif clair. La déclaration à travers laquelle la personne concernée matérialise son consentement peut être orale ou écrite, y compris par voie électronique[72]. Il existe une grande variété de procédés qui permettent de recueillir le consentement univoque de la personne concernée en l'invitant à adopter une attitude active[73]. Ainsi, cocher des cases sur un site web, opter pour certains paramètres techniques d'une page

---

[68] Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679, op. cit.,* p. 19.

[69] Il existe évidemment beaucoup de situations, dorénavant proscrites, dans lesquelles le consentement était autrefois induit du comportement passif de la personne concernée. Ces situations font l'objet de nombreux développements dans la doctrine. *« Zo kunnen ondernemingen betrokkenen bijvoorbeeld niet per brief of e-mail informeren dat zij geacht worden met een (desgevallend nieuwe) verwerking in te stemmen indien zij niet binnen een bepaalde termijn aangeven dat zij zich hiertegen verzetten. Ook is het niet mogelijk om de privacyfuncties van een dienst, bijvoorbeeld een sociaal mediaplatform, standaard op een bepaald niveau in te stellen totdat de betrokkene zelf de stap zet om deze instellingen aan te passen tot een lager niveau van verwerking (bv. van "profiel zichtbaar voor iedereen" naar "profiel enkel zichtbaar voor vrienden"). Dergelijke vormen van "opt-out"-toestemming kunnen voortaan in strijd worden geacht met het begrip toestemming in de GDPR »* (Karel JANSSENS, et Marion NUYTTEN, « De Algemene Verordening Persoonsgegevens : van theorie naar praktijk », *R.D.C.-T.B.H.*, 2018/5, p. 412).

[70] Benjamin DOCQUIR, *Répertoire pratique du droit belge - Législation, Doctrine, Jurisprudence - Droit du numérique, op. cit.*, p. 429.

[71] Axel BEELEN, *op. cit.,* pp. 46-47 ; Yves POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.,* p. 8 et Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679, op. cit.,* pp. 20-21.

[72] Voy. le considérant 32 du Règlement général sur la protection des données (RGPD).

[73] Cécile DE TERWANGNE et Karen ROSIER, *op. cit.*, p. 125.

Internet[74], faire glisser une barre sur un écran, agiter la main devant une caméra intelligente, former un huit avec son smartphone[75], reproduire une forme sur un écran tactile ou entrer une séquence de chiffres sur un clavier sont autant de possibilités qui permettent à la personne concernée de manifester clairement son consentement[76].

3. Un consentement de qualité évalué à la lumière des principes généraux de la protection des données

Comme nous venons de le voir, un traitement de données à caractère personnel n'est licite que s'il se fonde sur au moins l'une des six hypothèses visées à l'article 6, §1er, du RGPD. Parallèlement à cette disposition, le RGPD regroupe en son article 5, §1er, plusieurs principes généraux qui s'imposent au responsable du traitement. Ces principes fixent des exigences de licéité, loyauté et transparence, de limitation des finalités, de minimisation des données, d'exactitude, de limitation de la durée de conservation et de sécurité[77]. Les causes de licéité déterminées à l'article 6 ne dispensent pas le responsable du traitement de respecter les principes généraux de l'article 5 du RGPD[78] de sorte que les deux dispositions doivent être lues conjointement[79]. Une fois que nous aurons présenté les grandes lignes de la relation entre les articles 5 et 6 du RGPD (3.1), nous constaterons que l'équilibre de ceux-ci est parfois délicat (3.2).

---

[74] Voy. le considérant 32 du Règlement général sur la protection des données (RGPD).

[75] Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679, op. cit.,* p. 19.

[76] Parmi toutes ces modalités concrètes, les cases à cocher et les boutons « j'accepte » sont de loin les plus répandus mais ils ne sont pas inévitables pour autant. Par exemple, ceux-ci sont en effet inadaptés aux conversations orales ainsi qu'aux personnes concernées qui souffrent de problèmes de vue importants. Par ailleurs, comme le note le Groupe de travail de l'article 29, la répétition d'un procédé identique installe une certaine lassitude auprès des personnes concernées qui en viennent à consentir machinalement au traitement de leurs données (voy. Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679, op. cit.,* p. 20). Nous pensons par conséquent qu'une plus grande variété de procédés pourrait mener à une prise de conscience renforcée des personnes concernées.

[77] L'analyse de ces six principes généraux dépasse le cadre de la présente contribution. Pour des commentaires approfondis sur cette matière, voy. notamment Benjamin DOCQUIR, *Vers un droit européen de la protection des données ?*, *op. cit.*, pp. 92-105 et Romain ROBERT et Chloé PONSART, « Le règlement européen de protection des données personnelles », *J.T.*, 2018/20, pp. 423-424.

[78] La Cour de justice de l'Union européenne a reconnu le lien étroit qui existe entre le respect des principes généraux et la vérification des bases de licéité au traitement dans un important arrêt du 24 novembre 2011. Elle considère ainsi que « tout traitement de données à caractère personnel doit, d'une part, être conforme aux principes relatifs à la qualité des données énoncés à l'article 6 de ladite directive et, d'autre part, répondre à l'un des six principes relatifs à la légitimation des traitements de données énumérés à l'article 7 de cette même directive » (C.J.U.E., 24 novembre 2011, *arrêt ASNEF et FECEMD c. Administracion del Estado*, C-468/10 et C-469/10, pt. 26). Bien que relatif aux articles 6 et 7 de la Directive 95/46/CE, cet enseignement de la Cour peut aisément être transposé aux articles 5 et 6 du RGPD. (Voy. également en ce sens C.J.C.E., 20 mai 2003, *arrêts Rechnungshof c. Österreichischer Rundfunk e.a.*, C−465/00, C−138/01 et C−139/01, pt. 65).

[79] Marc VAN OVERSTRAETEN et Sébastien DEPRÉ, « Le traitement automatisé des données à caractère personnel et le droit au respect de la vie privée en Belgique », *Rev. trim. dr. h.*, 54/2003, pp. 689-690 et Thierry LÉONARD et Yves POULLET, « La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la Directive 95/46/CE du 24 octobre 1995 », *J.T.*, 1999, p. 384.

3.1. Un consentement de qualité en tant que condition nécéssaire mais non suffisante au traitement de données

Dans l'hypothèse particulière d'une demande de consentement, le fait que ce dernier soit libre, spécifique, éclairé et parfaitement univoque ne signifie pas qu'un traitement soit d'office admissible pour autant. Le Groupe de travail de l'article 29 considère en effet que « l'obtention d'un consentement n'annule pas ou ne diminue pas de quelque façon que ce soit l'obligation imposée au responsable du traitement de respecter les principes relatifs au traitement énoncés dans le RGPD, notamment dans son article 5 concernant la loyauté, la nécessité, la proportionnalité ainsi que la qualité des données. Ainsi, même si le traitement de données à caractère personnel a reçu le consentement de la personne concernée, cela ne justifie pas la collecte de données excessives au regard d'une finalité spécifique de traitement, ce qui serait foncièrement abusif »[80]. Dans le même esprit, le Rapport explicatif de la Convention n°108+ dispose que « l'expression d'un consentement ne dispense pas de respecter les principes fondamentaux de la protection des données à caractère personnel énoncés au chapitre II de la Convention : la proportionnalité du traitement, par exemple, doit toujours être considérée »[81].

Il s'ensuit que les causes de licéité visées à l'article 6 du RGPD et à la tête desquelles se trouve le consentement sont des conditions nécessaires mais non suffisantes au traitement de données dès lors que les principes généraux de l'article 5 du RGPD doivent également être respectés[82]. En d'autres termes, avant d'exploiter des données à caractère personnel, le responsable du traitement doit réaliser le cumul de l'examen des deux dispositions précitées.

3.2. Vers une présomption de respect des principes généraux de la protection des données ?

La question s'est par ailleurs posée de savoir si un consentement de qualité peut réellement être rejeté au motif qu'un principe général n'est pas respecté. Théoriquement, un traitement auquel la personne concernée aurait consenti est illégal s'il ne respecte pas, du reste, l'un des principes généraux repris à l'article 5 du RGPD[83]. Cependant, la réalité sera certainement moins évidente compte tenu de la place qu'occupe le consentement dans le droit de la protection des données[84]. Ainsi se demande-t-on dans quelle mesure un juge serait-il prêt à remettre en cause le sacro-saint consentement, véritable consécration du droit à l'autodétermination informationnelle, en

---

[80] Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679, op. cit.,* p. 3.

[81] Rapport explicatif de la version modernisée de la Convention n°108 du Conseil de l'Europe, adopté le 18 mai 2018, p. 22. Document disponible sur https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726, site consulté le 3 avril 2020.

[82] Yves POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.,* p. 21.

[83] Cécile DE TERWANGNE et Quentin VAN ENIS, *L'Europe des droits de l'homme à l'heure d'Internet,* Bruxelles, Bruylant, 2019, p. 339.

[84] Yves POULLET, *La vie privée à l'heure de la société du numérique*, *op. cit.*, pp. 129-130.

raison d'une atteinte, plus ou moins grande, à l'un des principes généraux de l'article 5 du RGPD ?

Notre quotidien est pourtant parcouru de nombreuses situations concrètes qui illustrent le délicat équilibre entre le consentement et les principes généraux. Par exemple, c'est notamment le cas lorsqu'un service de *streaming* musical tel que Spotify, Deezer ou Youtube Music collecte des données relatives aux heures et au volume d'écoute, aux types de chansons entendues, au lieu d'où la personne concernée se connecte ou à l'historique de ses recherches afin de lui recommander des morceaux qu'elle serait susceptible d'écouter, et ce, sur la base de son seul consentement. Dans ces conditions, nous sommes en droit de nous demander si le traitement de toutes ces données est proportionné ou non[85]. Par ailleurs, le traitement de multiples données, parfois très intimes, par des assistants personnels intelligents tels que Siri, Google Assistant, Alexa ou Cortana est-il bel et bien compatible avec le principe de minimisation des données consacré à l'article 5, §1er, c), du RGPD ?

Quoi qu'il en soit, il est clair que ces données sont devenues extrêmement précieuses — pour ne pas dire indispensables — à certaines sociétés du numérique. Il faut dès lors s'attendre à ce que celles-ci n'hésitent pas à brandir la preuve d'un consentement libre, spécifique, éclairé et univoque pour contester les reproches qui leur seraient adressés. Au lieu d'être examinés conjointement, les articles 5 et 6 du RGPD seraient alors opposés l'un à l'autre, ce qui n'est pas souhaitable. Au vu de ces constatations, nous en arrivons à nous demander si le surcroît de légitimité qui caractérise la conception actuelle du consentement n'est pas de nature à emporter une présomption de respect des principes généraux de la protection des données ?[86]

Il arrive toutefois que certains juges nationaux s'emploient courageusement à rétablir l'équilibre entre le consentement et les principes fondamentaux[87]. Généralement, les décisions qu'ils adoptent sont ensuite largement commentées par la doctrine[88].

4. Le consentement des mineurs d'âge

Par rapport à la Directive 95/46/CE, le RGPD entend protéger davantage les enfants dont les données à caractère personnel font l'objet d'un traitement[89]. Les enfants sont particulièrement

---

[85] Yves POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.,* p. 20.

[86] *Ibid.* pp. 20-21.

[87] Dans une récente affaire concernant le réseau social *Facebook*, un juge de la section néerlandophone du tribunal de première instance de Bruxelles a ainsi reconnu que plusieurs principes clés du traitement ont été violés par la multinationale. Il s'agissait en l'occurence des principes de loyauté, de finalité et de proportionnalité (voy. Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n°2016/153/A, *R.D.T.I.*, 2019/1, pp. 71 et s.).

[88] Voy. notamment Alejandra MICHEL, « Le traçage comportemental des internautes sur les réseaux sociaux : l'affaire des *"cookies Facebook"*, véritable saga judiciaire ? », *R.D.T.I.*, 2019/1, pp. 72-92 et Karen ROSIER, Coline FIEVET, Loïck GERARD, Odile VANRECK, Alejandra MICHEL, Julie MONT, Manon KNOCKAERT, Noémie GILLARD et Thomas TOMBAL, « Droit au respect de la vie privée et à la protection des données en lien avec les technologies de l'information - Chronique de jurisprudence 2015-2017 », *R.D.T.I.*, 2017/3-4, pp. 94-163.

[89] Cécile DE TERWANGNE et Karen ROSIER, *op. cit.*, p. 128.

vulnérables (4.1.) et c'est pourquoi le RGPD a renforcé leur protection lorsqu'ils sont invités à consentir au traitement de leurs données à caractère personnel dans le domaine des services de la société de l'information (4.2.).

4.1. Vulnérabilité des mineurs dans l'environnement numérique

Les mineurs sont des adultes en devenir qui, en raison de leur manque d'expérience et de maturité, doivent bénéficier d'une attention particulière matérialisée par un statut juridique distinct[90]. Leur vulnérabilité est renforcée lorsqu'ils se rendent sur Internet car ils ne sont pas toujours conscients des risques auxquels ils s'exposent. Ainsi, les enfants issus de la génération 2.0. qui recourent aux outils numériques de plus en plus tôt[91], représentent des proies faciles pour les structures spécialisées dans la collecte et le traitement des données à caractère personnel. Dans ce contexte, il est essentiel de protéger les mineurs de leurs propres faiblesses ainsi que de la possible malveillance des autres[92].

Soucieux du cas des mineurs, le RGPD a établi un niveau de protection supplémentaire à l'égard des enfants dont les données à caractère personnel sont traitées[93]. Le considérant 38 du RGPD précise en ce sens 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 »[94]. En outre, pour que leur protection soit optimale, il faut naturellement que les informations qui leur sont transmises soient exprimées en des termes clairs et simples[95]. Ces intentions sont spécifiquement formalisées au sein de l'article 8 du RGPD qui introduit un régime particulier au bénéfice des enfants qui manifestent leur consentement dans le domaine des services de la société de l'information.

4.2. Le régime spécifique du consentement exprimé par des mineurs dans le domaine des services de la société de l'information

L'article 8, §1er, du RGPD dispose que dans le contexte de l'offre de services de la société de l'information (4.2.1.), le traitement des données à caractère personnel auquel un enfant aurait consenti n'est licite que si l'enfant en question a dépassé l'âge minimum du consentement numérique. Loin d'être uniforme au sein de l'Union européenne, la fixation de cet âge minimum est, dans certaines limites, laissée à la discrétion des États membres (4.2.2.).

---

[90] Yves-Henri LELEU, *Droit des personnes et des familles*, 3e éd., Bruxelles, Larcier, 2016, p. 583.

[91] Karen ROSIER, « Les réseaux sociaux et les jeunes : la Commission européenne exhorte à une protection renforcée de leur vie privée », *B.J.S.*, 2011/460, p. 14.

[92] Hervé JACQUEMIN et Marc NIHOUL, *Vulnérabilités et droits dans l'environnement numérique*, Bruxelles, Larcier, 2018, p. 51.

[93] Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679, op. cit.,* p. 27.

[94] Considérant 38 du Règlement général sur la protection des données (RGPD).

[95] Voy. le considérant 58 du Règlement général sur la protection des données (RGPD).

4.2.1.Services de la société de l'information

L'article 8 du RGPD s'applique uniquement lorsque des services de la société de l'information sont directement offerts à des enfants[96]. L'article 4, 25°, du RGPD renvoie à la notion de service visée à l'article 1er, §1, b), de la Directive 2015/1535/UE[97] qui y est définie comme « tout service de la société de l'information, 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 »[98].

La Cour de justice de l'Union européenne estime par ailleurs que les offres en ligne ainsi que les contrats conclus par voie électronique sont couverts par la notion de service de la société de l'information. Il en va de même pour la fourniture d'un service sur Internet qui peut être considérée comme un service de la société de l'information au sens de l'article 8 du RGPD[99]. Il convient à ce titre de souligner que les services offerts par les réseaux sociaux constituent des services de la société de l'information[100] en ce qu'ils sont assimilables à des activités économiques, peu importe qu'ils soient rémunérés ou non par l'utilisateur[101].

4.2.2.L'âge du *« digital consent »*

L'article 8 du RGPD fixe un âge minimum à partir duquel le mineur est apte à manifester son *digital consent*. Selon cette disposition, dans le domaine des services de la société de l'information, le responsable du traitement qui souhaite exploiter les données à caractère personnel d'un mineur sur la base de son consentement doit s'assurer que celui-ci soit âgé d'au moins 16 ans pour que le traitement soit licite[102]. Dès lors, si le mineur a plus de 16 ans, il est capable de consentir seul au traitement de ses données. En revanche, s'il est âgé de moins de 16 ans, le traitement de ses données à caractère personnel ne pourra avoir lieu que si le responsable du traitement obtient l'accord d'un titulaire de la responsabilité parentale[103].

---

[96] Julie MONT, « R.G.P.D. : quelles nouvelles règles pour les enfants sur Facebook ? », *R.D.T.I.*, 2019/75, p. 9.

[97] 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.*, L 241 du 17 septembre 2015, p. 1.

[98] Article 1er, §1, b), de la Directive 2015/1535/UE.

[99] C.J.U.E., 2 décembre 2010, *arrêt Ker-Optika*, C-108/09, pts. 22 et 28.

[100] Si les services offerts par les réseaux sociaux constituent bel et bien des services de la société de l'information, l'inscription des enfants sur ces réseaux n'est toutefois pas couverte par le régime spécifique de l'article 8 du RGPD. En effet, « l'accès [aux réseaux sociaux] est (…) à dissocier de la question des données personnelles, qui est la seule réglementée par le RGPD » (Julie MONT, *op. cit.*, p. 6).

[101] Jean-Philippe MOINY, « Facebook au regard des règles européennes concernant la protection des données », *R.E.D.C.*, 2010/2, p. 240 et Julie MONT, *op. cit.*, p. 9.

[102] Cécile DE TERWANGNE et Karen ROSIER, *op. cit.*, p. 129.

[103] Sur la question de la représentation du mineur dans le contexte précis de l'article 8 du RGPD, voy. Nathalie MARTIAL-BRAZ, « Les nouveaux droits des personnes concernées », *R.A.E.-L.E.A.*, 2018/1, pp. 9-11.

Il faut par ailleurs noter que les États membres sont libres de prévoir par la loi un âge inférieur à 16 ans mais supérieur à 13 ans à partir duquel ils estiment que les enfants sont aptes à consentir au traitement de leurs données[104]. Cette flexibilité est le résultat d'une absence d'accord entre les États membres quant à la détermination de l'âge du consentement numérique. La latitude qui est ainsi laissée aux législateurs nationaux est regrettable dans la mesure où elle permet l'installation d'une hétérogénéité que les auteurs du RGPD ont pourtant cherché à éviter en adoptant un règlement plutôt qu'une directive[105]. Concrètement, le responsable du traitement qui offre des services de la société de l'information devra donc s'assurer que le mineur dont il recueille le consentement a dépassé l'âge minimum du consentement numérique au regard des différentes législations nationales[106].

5. Preuve du consentement

Aux termes de l'article 7, §1er, du RGPD, le responsable du traitement doit être en mesure de démontrer que la personne concernée a donné son consentement[107]. Une fois que la charge de la preuve qui repose sur le responsable du traitement aura été illustrée au moyen d'exemples concrets (5.1.), quelques commentaires seront consacrés aux procédures de certification. Celles-ci jouent un rôle essentiel pour répondre aux incertitudes que ressentent certains responsables du traitement quant à la comptabilité de leurs méthodes d'archivage avec le RGPD (5.2.).

---

[104] Alain BENSOUSSAN, *La protection des données personnelles de A à Z*, Bruxelles, Bruylant, 2017, p. 110 et Julie MONT, *op. cit.*, p. 10.

[105] Cécile DE TERWANGNE et Karen ROSIER, *op. cit.*, p. 130.

[106] Notons par exemple que le législateur belge a usé de la faculté offerte par le RGPD, puisque l'article 7 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel abaisse l'âge du consentement numérique à 13 ans. L'Autorité de protection des données a soutenu le choix du législateur en considérant que « cet âge correspond mieux à la réalité quotidienne de très nombreux jeunes qui surfent déjà sur Internet à un jeune âge » et qu'il faut éviter de les « priver d'opportunités de s'épanouir numériquement » (Autorité de protection des données, « RGPD : la limite d'âge de 13 ans correspond à la pratique numérique », Communiqué de presse du 13 février 2018, document disponible sur https://www.autoriteprotectiondonnees.be/news/rgpd-la-limite-dage-de-13-ans-correspond-a-la-pratique-numerique, site consulté le 6 avril 2020). Il n'en va pas de même en France où la loi du 20 juin 2018 relative à la protection des données personnelles opte, en son article 20, pour l'âge de 15 ans. Pour de plus amples détails concernant l'âge du consentement numérique à travers les États membres de l'Union, nous renvoyons aux résultats de la récente étude réalisée par l'Université de Gand, *« Status quo regarding the child's article 8 GDPR age of consent for data processing across the EU »,* document disponible sur https://www.betterinternetforkids.eu/en_US/web/portal/practice/awareness/detail?articleId=3017751, site consulté le 6 avril 2020.

[107] Voy. également le considérant 42 du Règlement général sur la protection des données (RGPD) qui dispose que « lorsque le traitement est fondé sur le consentement de la personne concernée, le responsable du traitement devrait être en mesure de prouver que ladite personne a consenti à l'opération de traitement ».

5.1. Charge de la preuve et illustrations concrètes

La charge de la preuve qui repose sur le responsable du traitement est double[108]. En effet, au-delà du devoir de prouver l'existence du consentement, le responsable du traitement doit par ailleurs se réserver la preuve que les exigences de qualité du consentement imposées par le RGPD ont bel et bien été rencontrées[109]. Il s'agit là d'une application du principe d'*accountability*[110] qui joue un rôle très important dans le cadre règlementaire de l'Union en matière de protection des données.

Que ce soit dans son registre des traitements ou dans un registre séparé, le responsable du traitement doit conserver une trace des principaux éléments qui lui permettront, le cas échéant, de prouver que ses opérations de traitement se fondent sur un consentement de qualité[111]. Afin d'établir la teneur de la demande de consentement, il peut notamment archiver une copie du formulaire de collecte accompagné de la *privacy policy* en vigueur à l'époque où le consentement a été donné[112]. En outre, pour que la preuve d'un consentement soit complète, le responsable du traitement doit prendre acte du moment auquel le consentement a été donné ainsi que l'identité de la personne concernée par le traitement[113]. Enfin, le responsable du traitement doit être en mesure de prouver de quelle façon la personne concernée a consenti au traitement. Si le consentement est donné de façon verbale, au cours d'un entretien téléphonique, il est possible de conserver un enregistrement de la conversation bien que l'archivage daté des notes prises par l'opérateur soient suffisantes pour prouver le consentement[114]. Si le consentement est donné en ligne, il est conseillé de stocker les données transmises en leur appliquant un horodatage nécessaire à leur identification[115].

---

[108] Alain BENSOUSSAN, *Règlement européen sur la protection des données, textes, commentaires et orientations pratiques*, Bruxelles, Larcier, 2016, pp. 94 et s.

[109] Yves POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.,* p. 9.

[110] Le principe d'*accountability* — ou de responsabilité — renvoie aux diverses obligations auxquelles tout responsable du traitement doit se conformer afin de démontrer qu'il respecte les exigences contenues dans le RGPD (Benjamin DOCQUIR, *Vers un droit européen de la protection des données ?*, *op. cit.*, p. 105). Ce principe, explicitement repris à l'article 5, §2, du RGPD, occupe une place centrale dans le contexte de la preuve d'un consentement de qualité. (Voy. en ce sens Autorité de protection des données, « Le nouveau règlement opère un changement important par rapport à la Directive 95/46 et prône le principe de l'*accountability* (ou de responsabilité) », document disponible sur https://www.autoriteprotectiondonnees.be/principe-de-responsabilite-accountability, site consulté le 8 avril 2020).

[111] Axel BEELEN, *op. cit.,* p. 51.

[112] Benjamin DOCQUIR, *Répertoire pratique du droit belge - Législation, Doctrine, Jurisprudence - Droit du numérique, op. cit.*, p. 430.

[113] La preuve de l'identité de la personne concernée n'implique pas nécessairement que son nom soit collecté. Un identifiant ou un nom d'utilisateur en ligne sont suffisants pour autant qu'ils permettent l'identification de la personne qui consent au traitement de ses données.

[114] Information Commissioner's Office (UK), « Consultation : GDPR consent guidance », 31 mars 2017, pp. 33-34. Document disponible sur https://iapp.org/media/pdf/resource_center/ICO-gdpr-consent-guidance.pdf, site consulté le 8 avril 2020.

[115] *Ibid.* p. 34.

5.2. L'importance des procédures de certification dans le contexte de l'aménagement de la preuve d'un consentement de qualité

Les responsables du traitement sont libres de développer les méthodes qu'ils estiment les plus appropriées pour prouver qu'ils ont recueilli un consentement de qualité conformément aux impératifs du RGPD. Cette liberté qui est laissée au responsable du traitement pour l'aménagement de la preuve ne doit cependant pas entrainer des volumes de traitement supplémentaires excessifs. Cela signifie qu'il ne faut pas collecter plus de données que celles qui sont strictement nécessaires à la preuve de l'obtention d'un consentement de qualité. De plus, l'archivage des données n'est plus autorisé à partir du moment où l'activité de traitement prend fin[116]. En pratique, ces exigences liées à la conservation des données génèrent un sentiment d'incertitude chez la plupart des responsables du traitement qui doutent que leurs méthodes soient suffisamment conformes au RGPD[117].

Dans ce contexte, les procédures de certification permettent de lever cette incertitude. Afin de s'assurer qu'elles collectent les informations avec une rigueur suffisante, les organisations publiques et privées peuvent mettre en œuvre un système de management de la protection de la vie privée conformément à une norme internationale de référence adoptée par un organisme de normalisation indépendant. À la suite de cette mise à niveau préalable, ces mêmes organisations peuvent entamer une démarche de certification de leur système auprès d'un organisme d'audit agréé, plus connu sous son appellation anglaise de *national Competent Body*. Si l'audit ne soulève aucune non-conformité majeure, l'organisme certificateur délivre un certificat. Ce dernier a une date de validité limitée de sorte qu'il doit être régulièrement renouvelé, à l'issue d'une nouvelle procédure d'audit.

Dans le domaine de la protection et de la collecte des données à caractère personnel la norme internationale la plus incontournable pouvant donner lieu à un audit de certification est la norme ISO/IEC 27701[118]. Publiée en août 2019, il s'agit de la première norme internationale qui traite du management de la protection de la vie privée. Sa mise en œuvre vise à permettre aux organisations d'évaluer, de traiter et de réduire les risques liés, entre autre, à la collecte de données[119]. Concrètement, l'organisation qui se prévaut d'une certification ISO/IEC 27701 est assurée de faire preuve d'un niveau élevé d'exigence en ce qui concerne ses opérations de

---

[116] Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679, op. cit.,* pp. 23-24.

[117] Informations recueillies le 7 avril 2020 auprès de Monsieur François GADISSEUR, délégué à la protection des données au sein du Parlement de Wallonie. Voy. également en ce sens Benjamin DOCQUIR, *Répertoire pratique du droit belge - Législation, Doctrine, Jurisprudence - Droit du numérique, op. cit.*, p. 437.

[118] Norme ISO/IEC 27701:2019, « Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices », résumé de la norme disponible sur https://www.iso.org/fr/standard/71670.html, site consulté le 8 avril 2020.

[119] PECB, « ISO/IEC 27701 - Système de management de la protection de la vie privée », analyse descriptive de l'organisme de certification, document disponible sur https://pecb.com/fr/education-and-certification-for-individuals/iso-iec-27701, site consulté le 8 avril 2020.

traitement et de collecte de données à caractère personnel[120]. Bien que la norme ISO/IEC 27701 n'ait pas exactement le même périmètre que le RGPD, la procédure de certification qui en découle est, à n'en pas douter, une bonne manière de prouver que certaines obligations contenues dans le RGPD sont pleinement remplies.

6. Retrait du consentement

Toute personne qui a consenti au traitement de ses données peut, à tout moment, retirer son consentement. Dans un premier temps, quelques développements seront consacrés aux conditions qui entourent l'exercice du retrait du consentement (6.1.). Les effets produits par le retrait seront ensuite envisagés, sans oublier d'y associer les conséquences d'un éventuel recours au droit à l'oubli (6.2.).

6.1. Conditions au retrait du consentement

L'article 7, §3, du RGPD dispose que toute personne dont les données sont traitées a le droit de retirer son consentement à tout moment, aussi simplement qu'elle l'a donné. Le Groupe de travail de l'article 29 précise, à cet égard, qu'il n'est pas nécessaire que le retrait du consentement se fasse par une action identique à celle qui a permis son expression[121]. Toutefois, il est à tout le moins hautement recommandé d'autoriser le retrait du consentement par le biais du même moyen de communication que celui par lequel le consentement a préalablement été donné[122]. En outre, les personnes concernées qui souhaitent retirer leur consentement doivent pouvoir le faire sans subir de préjudice d'aucune sorte. Le retrait doit ainsi être gratuit et il ne peut pas entrainer de diminution du niveau de service[123]. Si ces conditions[124] ne sont pas respectées, alors c'est la validité de l'ensemble du consentement qui est remise en cause.

À côté de l'hypothèse d'un retrait volontaire, le RGPD ne prévoit pas une période de péremption du consentement. Ce dernier ne sera donc jamais automatiquement retiré. Néanmoins, il ressort du caractère spécifique et éclairé du consentement qu'il est préférable

---

[120] Informations recueillies le 7 avril 2020 auprès de Monsieur François GADISSEUR, délégué à la protection des données au sein du Parlement de Wallonie. Notons que les Services du Parlement de Wallonie sont certifiés ISO/IEC 27001 (et non ISO/IEC 27701). La norme ISO/IEC 27001 assure « le management de la sécurité d'actifs sensibles tels que les données financières, les documents de propriété intellectuelle, les données relatives au personnel ou les informations confiées par des tiers ». Norme ISO/IEC 27001 « management de la sécurité de l'information », résumé de la norme disponible sur https://www.iso.org/fr/isoiec-27001-information-security.html, site consulté le 8 avril 2020.

[121] Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679, op. cit.,* p. 25.

[122] Benjamin DOCQUIR, *Vers un droit européen de la protection des données ?*, *op. cit.*, p. 95.

[123] Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679, op. cit.,* p. 25.

[124] Rappelons que le responsable du traitement est par ailleurs tenu d'informer la personne concernée de son droit à retirer son consentement. Il s'agit d'une des informations essentielles qui doit être communiquée avant que la personne concernée ne donne son consentement pour que ce dernier soit considéré comme suffisamment éclairé.

que celui-ci soit régulièrement renouvelé, notamment lorsque la finalité du traitement évolue. Il ne s'agit toutefois que de recommandations générales de bonne conduite qui ne sont pas explicitement visées par le RGPD[125].

6.2. Effets du retrait du consentement

La possibilité qui est offerte à la personne concernée de retirer son consentement — qu'il soit explicite ou non — à tout moment, rend celui-ci instable et précaire[126]. De surcroît, même si le retrait du consentement ne compromet pas la licéité du traitement effectué avant ce retrait[127], l'article 17 du RGPD offre à la personne concernée le droit d'obtenir du responsable du traitement, dans les meilleurs délais, l'effacement des données la concernant qui auraient jusqu'alors été collectées[128]. En d'autres termes, le responsable du traitement qui choisit de traiter des données à caractère personnel sur la base du consentement s'expose à deux risques majeurs. D'une part, il est susceptible de se retrouver inopinément sans fondement légal pour poursuivre ses activités de traitement[129]. D'autre part, la personne concernée peut exercer son droit à l'oubli et ainsi contraindre le responsable du traitement à effacer les données collectées à condition qu'il n'existe pas d'autre fondement juridique au traitement[130]. Par conséquent, afin de favoriser la stabilité des opérations de traitement, nous encourageons les responsables du traitement à n'utiliser le consentement qu'à titre subsidiaire, lorsqu'aucune autre base de licéité n'est envisageable.

---

[125] Benjamin DOCQUIR, *Répertoire pratique du droit belge - Législation, Doctrine, Jurisprudence - Droit du numérique, op. cit.*, p. 437.

[126] Axel BEELEN, *op. cit.,* p. 46.

[127] Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679, op. cit.,* p. 26.

[128] Voy. l'article 17, §1er, b), du Règlement général sur la protection des données (RGPD).

[129] Cécile DE TERWANGNE et Karen ROSIER, *op. cit.*, p. 128.

[130] Précisons d'emblée que certaines données peuvent être nécessaires à l'exercice de plusieurs traitements qui poursuivent différentes finalités et reposent sur des bases juridiques distinctes. Dans ce cas, le retrait du consentement n'emporte pas l'effacement des données dont le traitement se fonde sur une autre base juridique telle que le contrat ou l'intérêt légitime. Cette situation est à distinguer de celle où le responsable du traitement souhaite continuer à traiter les données à caractère personnel en substituant la base juridique du consentement à un autre fondement. Ici, le responsable du traitement « ne peut silencieusement passer du consentement (qui est retiré) à cet autre fondement juridique. Toute modification de la base juridique du traitement doit être notifiée à la personne concernée conformément aux exigences en matière d'information définies aux articles 13 et 14 et en vertu du principe général de transparence » (Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679, op. cit.,* p. 26).

TITRE 3. — LE CONSENTEMENT CONFRONTÉ AU DÉVELOPPEMENT DU NUMÉRIQUE ET DES INNOVATIONS TECHNOLOGIQUES : VERS LA FIN D'UN MYTHE ?

1. L'érosion progressive du consentement

Depuis son introduction dans le droit de l'Union européenne par la Directive 95/46/CE, le consentement, en tant que base de licéité au traitement s'est généralisé jusqu'à devenir le pilier essentiel sur lequel s'appuie le droit de la protection des données[131]. À l'origine, dans un contexte général où l'individu est placé au centre des nouvelles libertés consacrées à l'échelle européenne, le consentement s'est naturellement imposé comme la représentation la plus évidente du droit à l'autodétermination informationnelle. Si depuis lors les raisons qui justifient le recours au consentement sont restées inchangées, il convient d'observer que la société a quant à elle profondément évolué au gré des innovations technologiques. À cet égard, force est de constater que le consentement s'adapte difficilement aux nouveaux enjeux qui accompagnent l'inexorable essor du numérique[132].

L'environnement numérique facilite l'exploitation massive[133] de données à caractère personnel dans de multiples domaines. Les vidéos partagées sur un réseau social, les données de géolocalisation, les transactions bancaires, l'historique des achats en ligne, les termes insérés dans un moteur de recherche, les informations collectées par des objets connectés ou encore les images nécessaires à l'utilisation d'un logiciel de reconnaissance faciale sont autant d'exemples qui illustrent la grande variété de données susceptibles d'être traitées. Même si ces

---

[131] Yves POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.,* p. 4.

[132] D'après une étude prospective liée à l'univers numérique, celui-ci devrait rapidement peser plus de 44.000 milliards de gigaoctets de données. À l'horizon de l'année 2025, toute personne suffisamment à l'aise dans l'environnement numérique devrait interagir avec des objets connectés au moins une fois toutes les 18 secondes, ce qui représente 4800 interactions par jour. Ce constat est d'autant plus préoccupant que « all this data from new sources open up new vulnerabilities to private and sensitive information. There is a significant gap between the amount of data being produced today that requires security and the amount of data that is actually being secured, and this gap will widen — a reality of our data-driven world. By 2025, almost 90% of all data created in the global datasphere will require some level of security, but less than half will be secured ». (David REINSEL, John GANTZ et John RYDNING, « Data Age 2025 : The Evolution of Data to Life-Critical - Don't Focus on Big Data ; Focus on the Data That's Big », IDC, 2017, pp. 3-4. Document disponible sur https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/workforce/Seagate-WP-DataAge2025-March-2017.pdf, site consulté le 16 avril 2020).

[133] La collecte et la conservation de données dont la quantité croît de manière exponentielle est généralement désignée sous l'appellation de *big data,* ou de mégadonnées. Ce concept est généralement défini comme des « corps de données trop vastes (volume), trop divers en sources et en formats (variété) et trop rapidement produits (vitesse) pour être traités par les moyens habituels ». (Voy. Fanny COTON et Pauline LIMBRÉE, « Les données, des armes de déduction massive (données massives, recherche scientifique, profilage et décision automatisée à l'ère du Règlement Général sur la Protection des Données) » *in* Alexandre CASSART (coord.), *Le droit des MachinTech (FinTech, LegalTech, MedTech...)*, Bruxelles, Larcier, 2018, p. 10). Soulignons que la notion de *big data* ne doit pas être confondue avec le *cloud computing* ou le *data mining* qui renvoient respectivement au recours à des ressources extérieures d'une part, et à l'exploitation du *big data,* c'est à dire à l'exploitation d'une quantité phénoménale de données d'autre part. (Voy. Hervé JACQUEMIN et Marc NIHOUL, *op. cit.,* p. 347).

données, prises individuellement, n'ont que peu de valeur, elles en gagnent davantage lorsqu'elles sont croisées et imbriquées avec d'autres données[134].

En ligne, là où les demandes de consentement au traitement de données sont nombreuses, les personnes concernées ne manifestent que trop rarement un consentement de qualité. Selon l'expression imagée d'Emmanuel NETTER, elles ont en effet tendance à « foncer comme un taureau furieux »[135] vers le service proposé, sans prendre conscience de ce à quoi elles s'engagent réellement. Cette attitude peut difficilement leur être reprochée compte tenu de l'impossibilité pratique de concevoir un examen minutieux des *privacy policies* de chaque site web qu'elles consultent au moment de consentir au traitement de leurs données. En outre, il ne faut pas sous-estimer le caractère nécessaire — ou rendu nécessaire par la pression sociale — de certains services en ligne. Afin de préserver une vie sociale qui s'est désormais largement répandue sur les réseaux, les personnes concernées sont bien souvent forcées de consentir à tout prix au traitement de leurs données sans s'arrêter aux risques qu'elles prennent. Dans de telles hypothèses, le consentement se révèle être une protection en trompe-l'œil qui entretient l'illusion que toute personne concernée disposerait d'un contrôle absolu sur le traitement de ses données[136].

À l'ère du numérique, le droit de la protection des données est indispensable pour protéger les individus contre les risques auxquels les exposent les traitements de données. Face aux nouvelles technologiques de l'information et de la communication, les personnes concernées sont vulnérables[137]. Conscient de ces risques, le législateur européen a adopté de nouvelles exigences quant à la qualité du consentement au traitement de données. Ces précautions sont justifiées mais nous doutons, comme d'autres[138], qu'elles seront suffisantes pour relever les défis qui seront posés par l'évolution des moyens technologiques[139]. C'est pourquoi nous pensons que la seule solution durable qui parvienne à concilier la protection des données et le traitement de celles-ci dans un environnement numérique passe nécessairement par une érosion progressive du consentement, au bénéfice des autres bases de licéité qui sont d'ores et déjà visées par le RGPD.

---

[134] Fanny COTON et Pauline LIMBRÉE, *op. cit.*, p. 10.

[135] Emmanuel NETTER, « Sanction à 50 millions d'euros : au-delà de Google, la CNIL s'attaque aux politiques de confidentialité obscures et aux consentements creux », *Dalloz IP/IT*, 2019, p. 170.

[136] Yves POULLET, *La vie privée à l'heure de la société du numérique*, *op. cit.*, pp. 128-129.

[137] Hervé JACQUEMIN et Marc NIHOUL, *op. cit.,* p. 347.

[138] Voy. notamment Thierry LÉONARD, « Yves, si tu exploitais tes données », *in* Élise DEGRAVE, Cécile DE TERWANGNE, Séverine DUSOLLIER et Robert QUECK (dirs.), *Law, Norms and Freedoms in Cyberspace - Droit, normes et libertés dans le cybermonde - Liber Amicorum Yves POULLET*, Bruxelles, Larcier, 2018, p. 681 et Yves POULLET, *La vie privée à l'heure de la société du numérique*, *op. cit.*, p. 128.

[139] Comme le suggère Nadezhda PURTOVA, *« in the age of constant data collection and hundreds of data processing operations pertaining to one individual each day, it is believed that it is too much to ask of an individual to make truly informed decisions about each data processing operation, whether or not he or she wishes for his/her data to be processed »* (Nadezhda PURTOVA, « Do Property rights in personal data make sense after the big data turn ? », *Journal of Law and Economic Regulation,* 2017/10, p. 72).

2. Le consentement confronté aux innovations technologiques

L'environnement numérique représente un défi réel pour le droit de la protection des données. Au cœur de celui-ci, la place du consentement doit plus que jamais être réévaluée pour dégager des pistes de réflexion qui permettront d'envisager des solutions durables capables de protéger efficacement les utilisateurs des nouvelles technologies. À l'heure du *big data*, les *cookies* occupent une place centrale dans l'identification et le profilage des internautes. C'est pourquoi l'installation de *cookies* utilisés à des fins de traçage comportemental ne devrait être autorisée que si les utilisateurs d'Internet ont donné leur consentement, en pleine connaissance de cause (2.1.). Une fois les données recueillies, celles-ci sont traitées et exploitées par des technologies toujours plus performantes. Nous constaterons à cette occasion que le consentement prête de plus en plus le flanc à la critique (2.2.).

2.1. Le consentement au traçage du comportement en ligne au moyen de *cookies*

Au cours des dernières années, Internet n'a cessé de se développer jusqu'à devenir un outil incontournable de la société moderne. À mesure qu'Internet gagnait de l'importance dans nos vies, certains professionnels du secteur numérique ont doté leur site web de *cookies*, c'est à dire des petits fichiers enregistrés automatiquement dans le navigateur de l'utilisateur en vue de collecter des données sur celui-ci. Il existe une grande variété de *cookies* qui poursuivent des finalités distinctes. Loin d'être systématiquement inutiles ou dangereux, certains *cookies* sont nécessaires au fonctionnement des sites web. Ainsi, par exemple, il existe des *cookies* dont la finalité est d'assurer une meilleure sécurité et intégrité du site web. D'autres, en revanche, nettement plus dispensables, ont vocation à suivre les habitudes de navigation des internautes afin de les identifier pour leur proposer, le cas échéant, de la publicité ciblée[140]. Une fois collectées, ces données de navigation seront échangées et monnayées par des entreprises qui proposeront des annonces personnalisées aux utilisateurs de leur site en fonction de leurs goûts, de leurs envies et de leurs centres d'intérêt. L'importante collecte de données à laquelle certains *cookies* contribuent, alimente l'inexorable essor du *big data,* un phénomène qui met de plus en plus au défi le droit de la protection des données à caractère personnel.

Étant donné que l'utilisation de *cookies* permet le stockage et le traitement de données à caractère personnel, l'accord de la personne concernée est en principe requis[141]. Cet accord doit

---

[140] Sandrine CARNEROLI, *Marketing et internet*, Bruxelles, Larcier, 2011, p. 117.

[141] Notons que la CNIL considère que certaines catégories de *cookies* ne doivent pas nécessairement se fonder sur le consentement de l'utilisateur. Ainsi, « les *cookies* ayant pour finalité exclusive de permettre, ou de faciliter la communication par voie électronique et les *cookies* strictement nécessaires à la fourniture d'un service expressément demandé par l'utilisateur sont exonérés du recueil préalable de l'accord de l'internaute ». C'est notamment le cas des *cookies* de « panier d'achat », des *cookies* d'authentification, des *cookies* de *load balancing* ou encore des *cookies* persistants de personnalisation de l'interface utilisateur. (Guillaume DESGENS-PASANAU, *La protection des données personnelles - Le RGPD et la loi française du 20 juin 2018*, 4e éd., Paris, LexisNexis, 2019, p. 107).

être donné, en pleine connaissance de cause, après que l'utilisateur ait reçu une information claire et complète sur les finalités du dispositif[142]. À cet égard, l'Autorité de protection des données veille au grain. Le 17 décembre 2019, elle a par exemple infligé une amende de 15.000€ à une PME, de sa propre initiative, au motif que le site web de l'entreprise en question n'avait pas été configuré pour obtenir un consentement suffisamment granulaire qui s'étende aux différents types de *cookies*. En outre, le site web ne fournissait pas assez d'informations aux utilisateurs, notamment en ce qui concerne le droit de retirer leur consentement[143]. Les juridictions de l'ordre judiciaire n'hésitent pas non plus à montrer les muscles pour tenter de faire respecter le droit de la protection des données. Dans une récente affaire qui impliquait le géant américain *Facebook*, la chambre néerlandophone du tribunal de première instance de Bruxelles a ordonné, sous astreinte, la cessation de l'installation de *cookies* sur les terminaux des internautes tant que le réseau social se contenterait d'obtenir des consentements non valables de la part des utilisateurs, en considération des exigences de qualité du RGPD[144].

En matière de traçage comportemental sur Internet au moyen de *cookies*, les interventions accrues des autorités de contrôle, des juridictions nationales ainsi que de la Cour de justice de l'Union européenne[145] sont nécessaires. Toutefois, dans ce contexte, la question de l'efficacité du consentement que ces entités cherchent tant bien que mal à défendre, mérite d'être soulevée. En effet, quand on connaît les conséquences parfois très négatives que peuvent produire le traçage et le profilage en ligne, il convient de se demander si la seule garantie du consentement est à la hauteur des enjeux en cause. Le cas le plus incontournable qui illustre les dangers du profilage en ligne est sans aucun doute celui qui a impliqué l'entreprise Cambridge analytica et le réseau social *Facebook* dans le cadre des élections américaines de 2016. Dans cette affaire, il a été prouvé que les profils de plus de 50 millions d'américains ont été sondés et exploités par l'entreprise Cambridge analytica qui, sur la base de ces informations, s'est employée à diffuser des publications stratégiques dans le fil d'actualité des utilisateurs de *Facebook*, et ce, pour que le programme électoral de Donald TRUMP fasse mouche auprès du public ciblé[146].

---

[142] Guillaume DESGENS-PASANAU, *op. cit.*, pp. 104-105.

[143] Autorité de protection des données, chambre contentieuse, décision quant au fond 12/2019, 17 décembre 2019. Document disponible sur https://www.autoriteprotectiondonnees.be/decisions-de-la-chambre-contentieuse, site consulté le 20 avril 2020. Pour une analyse de cette décision et de ses effets, voy. Guillaume RUE, « L'autorité de protection des données impose une amende pour des *cookies* non conformes », *B.J.S.*, 2020/643, p. 11.

[144] Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n°2016/153/A, *R.D.T.I.*, 2019/1, pp. 71 et s. Pour une analyse détaillée de la décision, voy. Alejandra MICHEL, *op. cit.*, pp. 72-92.

[145] Notons par exemple que dans un récent arrêt, la C.J.U.E. a reconnu que le placement de *cookies* requiert le consentement actif des internautes. Ainsi, une case cochée par défaut n'implique pas un comportement actif de la personne concernée de sorte que les exigences de qualité du consentement ne sont pas rencontrées (C.J.U.E., 1er octobre 2019, *arrêt Planet49*, C-673/17). Pour de plus amples commentaires sur cet arrêt, voy. Guillaume RUE, « Le placement de cookies requiert le consentement actif des internautes », *B.J.S.*, 2019/639, p. 11 et Julie MEYER, Estelle DANTAN, Fanny LANGE, Célia GOURZONES et Elsa SADAKA, « La C.J.U.E. rejette la présomption de consentement au placement des *cookies* », *La revue des droits de l'homme* [en ligne], 2020, pp. 1 et s.

[146] Guido NOTO LA DIEGA, « Some Considerations on Intelligent Online behavioural Advertising », *R.D.T.I.*, 2017/66-67, p. 54.

Un autre problème se présente lorsque le site web qui requiert le consentement de ses utilisateurs n'a aucun concurrent sérieux ou que tous les concurrents fonctionnement sur un modèle de pseudo-gratuité, moyennant des publicités ciblées en contrepartie. Dans ces hypothèses, « le client n'a pas véritablement le choix et son consentement au contrat incluant des annonces personnalisées peut apparaître contraint »[147]. Une manière de résoudre cette difficulté pourrait consister à proposer des offres hybrides où l'accès au site serait soit gratuit et associé à de la publicité ciblée soit payant et dépourvu de toute forme de traçage. Quoi qu'il en soit, la politique de confidentialité des différents sites devra être parfaitement explicite pour permettre aux utilisateurs de choisir, en pleine conscience, l'offre qui leur convient le mieux[148].

2.2. Le consentement à l'épreuve des technologies du *big data*

Dans un contexte de collecte massive de données désigné sous l'appellation de *big data*, les techniques de *machine learning* sont des outils auxquels recourent certaines entreprises afin d'organiser et exploiter ces données à des fins commerciales. Après avoir introduit les notions d'intelligence artificielle, de *machine learning* et de *deep learning* (2.2.1.), nous présenterons les principales menaces qui pèsent sur les personnes concernées par le traitement de données, dans un environnement numérique, au moyen de quelques exemples concrets (2.2.2.). Ces illustrations nous permettrons d'expliquer, dans un second temps, ce en quoi l'état actuel du droit de l'Union européenne, et en particulier la notion de consentement, n'est plus adapté pour protéger efficacement les utilisateurs de nouvelles technologies (2.2.3.).

2.2.1. Intelligence artificielle, *machine learning* et *deep learning*

Définir la notion d'intelligence artificielle est une tâche complexe car elle est multidimensionnelle et protéiforme. On la rencontre en effet dans les domaines de l'informatique, de la science, des mathématiques et même de la philosophie. Par ailleurs, une telle aventure nécessiterait une approche technique détaillée qui dépasserait le cadre de la présente étude[149]. Ainsi nous limiterons-nous à reproduire les termes de la norme ISO/IEC 2382:2015 qui la définit comme la « capacité d'une unité fonctionnelle à exécuter des fonctions généralement associées à l'intelligence humaine comme le raisonnement et l'apprentissage »[150].

En complément de cette définition, il est tout de même utile de préciser que les intelligences artificielles peuvent être réparties en trois catégories distinctes selon leur niveau de maturité étalonné par référence aux performances d'un être humain. Une intelligence artificielle est

---

[147] Emmanuel NETTER, *op. cit.*, p. 171.

[148] *Ibid*.

[149] Pour une analyse fine et minutieuse de la notion d'intelligence artificielle nous renvoyons aux travaux d'Alain BENSOUSSAN et Jérémy BENSOUSSAN, « L'approche technique » *in IA, robots et droit*, Bruxelles, Bruylant, 2019, pp. 81 et s.

[150] Norme ISO/IEC 2382:2015, « Technologies de l'information - Vocabulaire », norme disponible sur https://www.iso.org/fr/standard/63598.html, site consulté le 16 avril 2020.

ainsi dite *faible* lorsqu'elle est tout au plus capable d'imiter un comportement humain sans chercher à comprendre ce qu'elle fait. L'algorithme est, dans ce cas, cantonné à une activité préalablement déterminée et totalement circonscrite. Au stade intermédiaire, l'intelligence artificielle est qualifiée de *forte* dès lors qu'elle est capable de réfléchir et d'agir comme le ferait un humain. Cette fois, elle n'est plus nécessairement guidée par des idées rationnelles et elle est susceptible de s'adapter au sein de l'environnement ouvert dans lequel elle évolue. Au sommet de cette catégorisation se trouvent les *super-intelligences* dotées d'un esprit qui dépasse de loin les capacités du cerveau humain et ce, dans tous les domaines[151]. Pour l'heure, de telles super-intelligences n'ont pas encore été créées et l'on se demande si elles le seront un jour quand on connaît la crainte — sans doute justifiée — qui accompagne la seule perspective de leur avènement.

La répartition ternaire qui précède se fonde sur le degré de raisonnement des intelligences artificielles. Elle implique une compréhension minimale des techniques d'apprentissage des algorithmes parmi lesquelles[152] on rencontre notamment le *machine learning*, dont le *deep learning* est une sous-catégorie[153]. Le *machine learning* se compose d'un ensemble d'algorithmes qui ont la capacité d'améliorer leurs compétences par l'analyse et le traitement de multiples données fournies en exemple, sans que soit nécessaire une intervention humaine systématique. En d'autres termes, l'algorithme de *machine learning* est conçu pour optimiser les paramètres des modèles utilisés grâce au traitement d'une grande quantité de données sans que son concepteur n'ait besoin d'identifier ces paramètres au préalable[154]. Le *deep learning* ou apprentissage profond, correspond pour sa part à une des techniques par lesquelles les algorithmes de *machine learning* traitent les données qui leur sont fournies. À l'image du réseau neuronal du cerveau humain, le *deep learning* utilise une plus grande quantité de couches de neurones artificiels que les autres techniques de *machine learning* afin de pouvoir traiter une quantité phénoménale de données d'entrée[155]. Dans ce contexte, face à l'appétit insatiable en données des technologies du *big data,* il convient de se demander si le consentement demeure une voie appropriée pour organiser le traitement des données de la personne concernée.

---

[151] Adrien VAN DEN BRANDEN, *Les robots à l'assaut de la justice - L'intelligence artificielle au service des justiciables,* Bruxelles, Bruylant, 2019, pp. 81-82.

[152] D'après un rapport issu de l'Office parlementaire d'évaluation des choix scientifiques et technologiques français, il existe trois formes d'apprentissage des algorithmes. Tout d'abord, l'apprentissage est dit *supervisé* lorsque l'algorithme « définit des règles à partir d'exemples qui sont autant de cas validés ». Ensuite, l'apprentissage est *non supervisé* si « le modèle est laissé libre d'évoluer vers n'importe quel état final lorsqu'un motif ou un élément lui est présenté ». Enfin, entre ces deux catégories, l'apprentissage est *automatique* s'il est « semi-supervisé ou partiellement supervisé ». Cette dernière hypothèse correspond au *machine learning.* (Voy. le Rapport de l'OPECST, « Pour une intelligence artificielle maîtrisée, utile et démystifiée », t. I, enregistré à la présidence de l'Assemblée nationale et du Séant le 15 mars 2017, pp. 48-49. Document disponible sur http://www.senat.fr/rap/r16-464-1/r16-464-11.pdf, site consulté le 16 avril 2020).

[153] Alain BENSOUSSAN et Jérémy BENSOUSSAN, *op. cit.*, p. 89.

[154] Adrien VAN DEN BRANDEN, *op. cit.,* p. 82.

[155] Liane CHANCERELLE, « La lutte contre les discriminations en Europe à l'ère de l'intelligence artificielle et du big data », *J.D.J.*, 2019/1, p. 26.

2.2.2. Les principaux défis du consentement à l'exploitation de données par des intelligences artificielles

Au cours des dernières années, de nombreux progrès ont été réalisés dans le domaine de l'intelligence artificielle. Celles-ci sont désormais capables de traiter de manière automatisée une quantité impressionnante de données à l'aide d'algorithmes de *machine learning*. Au départ des informations techniques de la section précédente, il convient à présent d'apporter une perspective plus concrète à la réflexion au moyen de deux innovations technologiques dont l'usage est voué à se généraliser, à savoir les *chatbots* d'une part (2.2.2.1.), et des robots d'autre part (2.2.2.2.). Nous en profiterons pour mettre en exergue la fragilité du consentement face aux défis qui accompagnent la place de plus en plus importante que de telles inventions ne manqueront pas d'occuper, à l'avenir, dans notre quotidien.

2.2.2.1. Les *chatbots*

Les *chatbots,* ou agents conversationnels, sont des applications d'intelligence artificielle qui permettent à des prestataires de services de dialoguer virtuellement, sans intervention humaine avec des utilisateurs humains[156]. Ces programmes, basés sur le stockage d'informations et l'utilisation d'algorithmes se rencontrent sous la forme de plateformes de messagerie instantanée ou, plus récemment, d'enceintes connectées. En quelques années, ces *chatbots* sont devenus très répandus au point de conquérir les espaces les plus intimes des utilisateurs[157]. Ils font l'objet d'usages variés dans divers domaines tels que le milieu bancaire[158], les ressources

---

[156] Patrick HENRY, « Fiona, Tina et le monde d'hier » *in* Jean DE CODT, Beatrijs DECONINCK, Dirk THIJS et Jean-François VAN DROOGHENBROECK (dirs.), *Le Code judiciaire a 50 ans. Et après ? / 50 jaar Gerechtelijk Wetboek. Wat nu ?*, Bruxelles, Larcier, 2018, p. 384.

[157] D'après une récente étude menée par Microsoft, les agents conversationnels domestiques les plus utilisés sont par ordre de préférence Google Assistant (36%), Siri d'Apple (36%), Alexa d'Amazon (25%) et Cortona de Microsoft (19%). L'étude ajoute que ces assistances vocales vont continuer à se répandre jusqu'à devenir véritablement incontournables dans la vie quotidienne. (Voy. Microsoft, « Voice report - From answers to action : customer adoption of voice technology and digital assistants », 2019, pp. 8 et s. Document disponible sur https://advertiseonbing-blob.azureedge.net/blob/bingads/media/insight/whitepapers/2019/04%20apr/voice-report/bingads_2019voicereport.pdf, site consulté le 18 avril 2020).

[158] Les banques confient de plus en plus de tâches aux *chatbots* qui jouent le rôle de conseillers virtuels. Nous pouvons, par exemple, citer les agents conversationnels « Erica » de la *Bank of America* ou encore « Eno » de la banque Capital One. (Alain BENSOUSSAN et Jérémy BENSOUSSAN, « Les chatbots » *in IA, robots et droit*, Bruxelles, Bruylant, 2019, p. 228).

humaines[159], la pratique notariale[160], le tourisme[161] ou encore les relations de travail[162]. Paradoxalement, le droit de la protection des données s'est lui-même ouvert aux agents conversationnels depuis la création d'« Eva », le premier *chatbot* en dialogue vocal entièrement dédié au RGPD[163].

Tout *chatbot* qui entre directement en contact avec un utilisateur est amené à recueillir des données sur celui-ci. Ainsi, les agents conversationnels vocaux font appel à plusieurs technologies avancées pour capter, analyser, et réagir aux paroles de l'utilisateur. Du point de vue du droit à la protection des données, il s'agit d'un défi de taille car les données biométriques de la personne concernée sont sujettes à d'importantes opérations de traitement. Dans ce contexte, outre le respect des impératifs de *privacy by design* et de *privacy by default,* les *chatbots* vocaux devront compter sur le consentement explicite de la personne concernée[164]. Par ailleurs, il se pourrait qu'un *chatbot* vocal ait pour finalité l'analyse de certains aspects personnels de la vie de l'utilisateur afin de prédire, par exemple, sa localisation, ses centres d'intérêt, ses déplacements, sa situation économique, sa santé, ses habitudes sportives, etc[165]. Si ces données, une fois traitées, aboutissent à une décision individuelle automatisée, la personne concernée peut s'y opposer sauf si cette décision est fondée sur son consentement explicite[166]. Dans ce contexte, compte tenu des réels dangers qui accompagnent le développement des *chatbots,* il convient de se demander si le consentement, fût-il même explicite, constitue une base suffisante pour fonder le traitement, la collecte et l'exploitation de données éminemment personnelles.

---

[159] Dans le domaine des ressources humaines, les *chatbots* sont de plus en plus utiles pour réaliser des tâches répétitives comme le suivi des congés et absences, la gestion des fiches de paie, le tri des CV, le contact de nouveaux collaborateurs potentiels, etc. (Alain BENSOUSSAN et Jérémy BENSOUSSAN, *op. cit.*, p. 229).

[160] Les premières intelligences artificielles qui ont pleinement intégré le monde notarial prennent la forme de *chatbots* disponibles en ligne. En Belgique, ces assistants virtuels sont d'ores et déjà opérationnels pour conseiller les justiciables qui auraient des questions relatives au droit des biens matrimoniaux ou au nouveau code de droit des sociétés et des associations (Paul DANNEELS, « Fundamenten voor een AI gedreven notariaat » in *Tradition in motion*, Gent, Larcier, 2019, p. 114).

[161] Le tourisme intelligent recourt généralement aux *chatbots* pour fournir aux voyageurs des informations en continu sur le voyage qu'ils entreprennent. En France, par exemple, le *chatbot* SNCF Transilien accompagne le voyageur à partir du moment où il a acheté son billet, jusqu'à la fin de son voyage (Alain BENSOUSSAN et Jérémy BENSOUSSAN, *op. cit.*, p. 228).

[162] Dans le cadre des relations de travail une startup a récemment développé un *chatbot* du nom de « Spot » qui est chargé de lutter contre les cas de harcèlement sexuel. Concrètement, les travailleurs se confient à l'agent conversationnel Spot qui examine si les faits qui lui sont communiqués sont susceptibles d'être sanctionnés par le droit pénal (Alain BENSOUSSAN et Jérémy BENSOUSSAN, *op. cit.*, pp. 228-229).

[163] Créée en mai 2018, Eva est un agent conversationnel vocal qui conseille les entreprises, les associations et les organes publics en leur fournissant des informations de premier ordre sur les dispositions du RGPD. (Alain BENSOUSSAN et Jérémy BENSOUSSAN, *op. cit.*, p. 229).

[164] Voy. l'article 9, §2, a), du Règlement général sur la protection des données (RGPD).

[165] Alain BENSOUSSAN et Jérémy BENSOUSSAN, *op. cit.*, pp. 234-235.

[166] Voy. l'article 22, §2, c), du Règlement général sur la protection des données (RGPD).

2.2.2.2.Les robots d'assistance domestique

La prochaine étape de l'évolution des intelligences artificielles sera matérialisée par l'avènement des robots. Ceux-ci peuvent prendre de multiples formes, poursuivre de nombreuses finalités, avoir des tailles variables, embarquer différents niveaux d'intelligence artificielle et évoluer dans des environnements distincts. Globalement, la notion de robot peut donc être définie comme toute « machine intelligente capable de prendre des décisions de manière libre, interagissant avec son environnement, dotée de mobilité, agissant en coopération avec les hommes et dotée d'une capacité d'apprentissage »[167]. Pour illustrer les principaux enjeux qui accompagnent l'arrivée des robots en droit de la protection des données, l'accent sera porté sur les robots d'assistance domestique dont le fonctionnement implique la collecte de vastes quantités de données à caractère personnel[168].

Les robots qui sont destinés à un usage domestique sont invités à aider, discuter et conseiller leurs utilisateurs. En accomplissant ces missions, d'apparence tout à fait anodines, les robots deviennent des confidents, des amis, voire même des familiers. Pour certains, il découle de ces nouvelles relations entre l'homme et la machine au moins six dangers flagrants : (1) le risque d'une surveillance accrue, (2) l'incursion dans des endroits jusqu'alors protégés, (3) la collecte invisible et permanente de données par des capteurs performants intégrés à la machine, (4) les éventuelles défaillances dans la cybersécurité du robot, (5) les attaches émotionnelles que l'homme entretiendrait à l'égard du robot ainsi que (6) le manque d'information des utilisateurs concernant le fonctionnement du robot ou de ses finalités[169].

L'usage de robots dans la vie quotidienne soulève, par ailleurs, la question du consentement de ses utilisateurs. En effet, dès les premiers contacts, afin d'interagir le plus naturellement possible avec son entourage, le robot a besoin de traiter des données à caractère personnel qui lui permettront de définir un service sur mesure[170], et ce, avant même qu'un consentement au

---

[167] Alain BENSOUSSAN et Jérémy BENSOUSSAN, *op. cit.*, p. 82.

[168] En ce qui concerne les robots d'assistance domestique, il convient d'être vigilant au champ d'application matériel du RGPD afin de déterminer si ce dernier s'applique ou non. En effet, l'article 2, §2, c), dispose que les dispositions du RGPD ne s'appliquent pas aux traitements effectués par une personne physique dans le cadre d'une activité strictement personnelle ou domestique. En d'autres termes, quand l'utilisateur du robot est aussi responsable du traitement, il est possible que le RGPD ne s'applique pas si le traitement en cause est exclusivement réalisé dans le cadre d'une activité domestique. En revanche, si le fabricant du robot est lui-aussi responsable du traitement et qu'il collecte des données pour son propre compte, il ne pourra pas se prévaloir de l'exception de l'article 2, §2, c). Par conséquent, les exigences du RGPD s'imposeront à lui.

[169] Voy. Antoine DELFORGE et Loïck GERARD, « Notre vie privée est-elle réellement mise en danger par les robots ? Étude des risques et analyse des solutions apportées par le GDPR », *in* Hervé JACQUEMIN et Alexandre DE STREEL (coord.), *L'intelligence artificielle et le droit*, Bruxelles, Larcier, 2017, pp. 143 et s.

[170] Yves POULLET, *La vie privée à l'heure de la société du numérique*, *op. cit.*, pp. 130-131.

traitement n'ait été formulé[171]. Si le robot a été conçu dans le respect du principe de *privacy by design*, il devra rapidement s'assurer d'obtenir le consentement éclairé de ses utilisateurs en les informant au préalable de la nature des données collectées ainsi que des finalités de leur traitement.

Outre l'importante réflexion sur la place du consentement dans la relation entre le robot et ses utilisateurs réguliers, il convient de relever que la situation est d'autant plus problématique lorsque ce robot entre en contact avec des tiers involontaires. S'il est possible d'obtenir le consentement des personnes qui fréquentent régulièrement le robot, il n'en va pas toujours de même pour toutes celles et ceux qui se contentent de graviter autour de l'environnement dans lequel le robot évolue. Pourtant, il est nécessaire que le robot mémorise des données sur les tiers qu'il rencontre de près ou de loin si l'on attend de lui une continuité dans la relation avec ces personnes, à l'avenir[172]. Ainsi, un robot qui serait chargé de s'occuper du jardin serait inévitablement amené à croiser des voisins ou des passants dans la rue sans pouvoir recueillir un consentement de qualité de leur part pour légitimer la collecte des différentes données qui les concernent. Pareillement, le robot-compagnon d'une personne âgée a besoin de collecter certaines informations relatives aux tiers tels que le timbre de la voix de l'infirmière à domicile, la fréquence des visites de celle-ci ou de tout autre membre de la famille, etc. Les illustrations sont nombreuses et elles aboutissent généralement au constat qu'en matière « de robots [et] de profilage, on pressent que la réponse individuelle que prône le consentement n'est pas adéquate lorsqu'il s'agit de légitimer de tels traitements »[173].

2.2.3.Inconsistance du consentement à l'heure des *big data*

L'importante masse de données qui se rapporte aux utilisateurs de nouvelles technologies dans un environnement numérique constitue la matière première de pratiques algorithmiques inédites de filtrage, de classification et de hiérarchisation des contenus informationnels[174]. En matière de protection des données à caractère personnel, le phénomène du *big data* comporte de nombreux risques[175]. Outre les différentes illustrations présentées dans la section précédente, le profilage numérique, le *personal tracking*, l'hyperindividualisation, l'opacité des algorithmes, l'émergence de nouvelles discriminations ou encore le spectre d'une surveillance

---

[171] Dès son activation, diverses données sont traitées par le robot. Comme le notent Antoine DELFORGE et Loïck GERARD, le robot a par exemple « besoin de filmer la personne ou d'enregistrer [les propos de celle-ci] pour vérifier s'il connaît déjà cette personne, d'analyser son ton de voix pour adapter ses propos à l'humeur de la personne… et tout ça avant même d'avoir commencé à véritablement discuter avec cette personne. Simplement pour vérifier que la personne a éventuellement déjà donné son consentement pour traiter des données la concernant, le robot va être amené à traiter des données personnelles ». (Antoine DELFORGE et Loïck GERARD, *op. cit.*, p. 172).

[172] Antoine DELFORGE et Loïck GERARD, *op. cit.*, pp. 172-174.

[173] Yves POULLET, *La vie privée à l'heure de la société du numérique*, *op. cit.*, p. 131.

[174] Antoinette ROUVROY, « Homo juridicus est-il soluble dans les données ? » *in* Elise DEGRAVE, Cécile de TERWANGNE, Séverine DUSOLLIER et Robert QUECK (dirs.), *Law, Norms and Freedoms in Cyberspace - Droit, normes et libertés dans le cybermonde - Liber Amicorum Yves POULLET*, Bruxelles, Larcier, 2018, p. 419.

[175] Miguel MAIRLOT, « Big Data et vie privée : mariage possible ? », *D.B.F.-B.F.R.*, 2015/6, p. 451.

de masse ne représentent qu'une fraction des différentes menaces auxquelles les utilisateurs de nouvelles technologies numériques seront directement exposés avec une intensité croissante[176].

Pour répondre aux enjeux de la société numérique, il est nécessaire que le droit de la protection des données évolue et s'adapte en conséquence, car il apparaît clairement que le cadre juridique actuel n'est pas en phase avec la réalité informatique. Ainsi, il semblerait que les grands principes européens de minimisation des données[177], de limitation de finalités[178] et de limitation de la conservation des données[179] sont condamnés à rester des vœux pieux précisément parce qu'ils entrent en opposition frontale avec les *big data.* En effet, comme le résume fort bien Antoinette ROUVROY, « les *big data,* au contraire de la minimisation, c'est la collecte maximale, automatique, par défaut, et la conservation illimitée de tout ce qui existe sous une forme numérique, sans qu'il y ait, nécessairement, de finalité établie *a priori* : l'utilité des données ne se manifeste qu'en cours de route, à la faveur des pratiques statistiques de *data mining*, de *machine learning,* etc., des données *a priori* inutiles peuvent se révéler extrêmement utiles à terme à des fins de profilage par exemple, et gagnent en utilité au fur et à mesure que grossissent les jeux de données »[180].

Dans le prolongement des réflexions qui précèdent, il est évident que l'évolution du droit de l'Union européenne est particulièrement nécessaire et souhaitable pour la notion de consentement. Comme d'autres[181], nous pensons en effet que dans un environnement hyperconnecté, la promesse d'un contrôle individuel sur l'ensemble de ses propres données est, en réalité, tout à fait illusoire : « ni le principe du consentement individuel au traitement des données personnelles, ni les systèmes les mieux intentionnés de *privacy by design* ne sont de nature à endiguer le tsunami de données »[182]. De plus, face aux risques importants qui accompagnent le développement du *big data*, nous considérons que le consentement, parfois creux et vide de sens, ne constitue plus une protection suffisante. À l'heure des *big data,* il faut rester vigilant au fait qu'un simple consentement peut constituer une ouverture à de nouvelles techniques de traitement. Concrètement, le défi qui se pose nous invite à réévaluer la place qu'il convient de donner au droit à l'autodétermination informationnelle dans un monde numérique où les données font l'objet de traitements constants, toujours plus performants.

---

[176] Antoinette ROUVROY, *op. cit.,* pp. 421-423.

[177] Article 5, §1, c), du Règlement général sur la protection des données (RGPD).

[178] Article 5, §1, b), du Règlement général sur la protection des données (RGPD).

[179] Article 5, §1, e), du Règlement général sur la protection des données (RGPD).

[180] Antoinette ROUVROY, *op. cit.,* p. 429.

[181] Voy. notamment Thierry LÉONARD, *op. cit.,* p. 681 et Yves POULLET, *La vie privée à l'heure de la société du numérique*, *op. cit.*, pp. 128-129.

[182] Antoinette ROUVROY, *op. cit.,* p. 430.

TITRE 4. — LA PLACE PRIVILÉGIÉE DU CONSENTEMENT COMME CAUSE DE LICÉITÉ AU TRAITEMENT : REMISE EN CAUSE ET PISTES DE RÉFLEXION

1. Le consentement, une notion dépassée ?

Au fil des années, le consentement, s'est progressivement imposé comme la pierre angulaire du droit européen de la protection des données, tant et si bien que certains n'hésitent pas à lui reconnaître, non sans une pointe de dérision, le rang quasi-spirituel de « dogme »[183]. À l'origine, si le consentement constituait sans doute la meilleure base juridique pour garantir la protection des données à caractère personnel de la personne concernée tout en lui reconnaissant un droit à l'autodétermination informationnelle, nous pensons qu'il n'en sera pas de même à l'avenir. En effet, nous constatons d'ores et déjà plusieurs signaux issus de la pratique et relayés par la doctrine qui révèlent les carences du consentement.

Comme nous l'avons précisé au titre précédent, le phénomène des *big data* qui accompagne la constante expansion de l'environnement numérique met le droit de la protection des données en crise[184]. Le traçage comportemental sur Internet au moyen de *cookies*, la collecte massive de données, le recours à de innovations technologiques embarquant des intelligences artificielles toujours plus performantes sont autant de défis que le législateur européen devra relever. Pour ce faire, certains pans du droit de la protection des données devront être reconsidérés. En ce qui concerne en particulier les bases de licéité au traitement, nous voyons à travers le durcissement des exigences de qualité du consentement introduit par le RGPD, les derniers soubresauts d'un système dépassé, qui a plus que jamais besoin d'être réinventé en profondeur.

Parmi ceux qui remettent en cause le poids du consentement au traitement de données à caractère personnel[185], Yves POULLET se demande pour sa part si « le mythe du consentement n'aboutit pas à la construction d'un cadre juridique qui affirme l'importance de la vie privée pour l'autonomie des sujets et, partant, la démocratie, mais qui laisse le poids de sa défense aux individus, à travers le concept de consentement individuel. L'individu est-il à suffisance armé pour réguler l'utilisation de données certes le concernant mais dont le traitement concerne également autrui voire l'intérêt général ? »[186] Cette réflexion nous amène à évaluer si la

---

[183] Ainsi, dans un récent article, Yves POULLET invite ses lecteurs à « remettre en cause le dogme du consentement au profit d'une réflexion plus collective sur les enjeux des traitements des données et la possibilité de juger de leur légitimité à l'aune de cette réflexion ». (Yves POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.,* p. 21).

[184] Pour un avis similaire voy. Antoinette ROUVROY, *op. cit.,* p. 427.

[185] À cet égard, nous renvoyons notamment aux travaux de Claire LOBET-MARIS et Julie COHEN qui qualifient toutes deux le consentement de *privacy bug*. (Voy. Claire LOBET-MARIS, « Du fétichisme de la donnée personnelle. Relecture politique et critique de la vie privée » *in* Élise DEGRAVE, Cécile de TERWANGNE, Séverine DUSOLLIER et Robert QUECK (dirs.), *Law, Norms and Freedoms in Cyberspace - Droit, normes et libertés dans le cybermonde - Liber Amicorum Yves POULLET*, Bruxelles, Larcier, 2018, p. 696 et Julie COHEN, « Privacy, Ideology and Technology », *The Georgetown Law Journal*, 2001/89, p. 2029).

[186] Yves POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.,* p. 37.

solution aux difficultés rencontrées dans la pratique en matière de consentement ne consisterait pas à envisager ce dernier selon une approche non pas purement individualiste mais bien collective.

2. Vers une approche collective du consentement ?

L'idée que le consentement serait l'élément clé du droit européen de la protection des données est désormais battue en brèche par une frange de plus en plus importante de la doctrine qui lui reproche notamment de buter sur des problèmes pratiques[187]. Confronté au développement du monde numérique, les critiques se renforcent[188] et les premières initiatives de réévaluation de la notion de consentement apparaissent peu à peu. L'une de celles-ci consisterait à abandonner la dimension individuelle du consentement au profit d'un consentement plus collectif, négocié en amont par le prestataire de services, le responsable du traitement ainsi qu'une ou plusieurs associations d'utilisateurs. Les autorités de contrôle nationales seraient également invitées à jouer un rôle direct dans la négociation via le Comité européen de protection des données[189]. Concrètement, cette proposition originale reviendrait à « soumettre les *privacy policies* à un consentement collectif qui fixerait ce qui est acceptable, ce qui est exclu et les marges de manœuvre laissées au prestataire et, peut-être au consentement individuel »[190].

Les tenants de cette approche collective considèrent qu'il s'agit là de la voie la plus indiquée pour répondre aux problèmes majeurs qui caractérisent l'approche purement individualiste du consentement. La première difficulté qu'ils identifient tient à « la réalité des consentements exprimés sur la toile, dont peu sinon aucun ne remplit les conditions légales [de sorte que] la pratique des consentements individuels présente une illusoire protection »[191]. Ils constatent par ailleurs qu'une approche subjective du consentement ne permet pas « d'opérer une prise en compte pleine et efficace de l'intérêt général et des risques collectifs que peuvent impliquer la mise en œuvre du marché des données qui serait ainsi volontairement alimenté par les personnes elles-mêmes sans garanties suffisantes »[192]. Ce sont ces observations qui poussent certains auteurs à penser que seule une négociation collective qui fixerait les limites du consentement individuel représenterait une solution efficace et durable.

L'approche collective du consentement est une idée audacieuse qui a le mérite de redéfinir les contours d'une notion qui a plus que jamais besoin d'être modernisée. Cependant, nous

---

[187] Voy. par exemple Lee BYGRAVE et Dag WIESE SCHARTUM, « Consent, Proportionality and Collective Power », *in* Serge GUTWIRTH, Yves POULLET, Paul de HERT, Cécile de TERWANGNE et Sjaak NOUWT (éds.), *Reinventing Data Protection ?*, Heidelberg, Springer, 2009, pp. 160-161. Les auteurs insistent notamment sur les difficultés d'obtenir un consentement pleinement informé ainsi que sur les situations de monopole qui ne permettent pas toujours à la personne concernée de manifester une volonté libre.

[188] Voy. notamment Nadezhda PURTOVA, *op. cit.*, p. 12.

[189] Yves POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.,* pp. 36-37.

[190] *Ibid*., p. 10.

[191] *Ibid*.

[192] Thierry LÉONARD, *op. cit.,* p. 681.

pensons que l'élément central qui fait la force de cette théorie rend également celle-ci impraticable, du moins en l'état actuel du droit. En effet, l'article 8 de la Charte des droits fondamentaux de l'Union européenne précise bien que les données à caractère personnel « doivent être traitées loyalement, à des fins déterminées et *sur la base du consentement de la personne concernée*[193] ou en vertu d'un autre fondement légitime prévu par la loi »[194]. En d'autres termes, reconnaître une dimension collective au consentement reviendrait sans doute à méconnaître l'esprit de la Charte qui, comme nous l'avons déjà indiqué, consacre précisément un droit à l'autodétermination informationnelle. Nous craignons donc qu'un glissement de l'approche subjective du consentement à une approche plus collective soit rapidement contestée par les juges de la Cour de justice de l'Union européenne qui devraient, logiquement, se ranger derrière la dimension individualiste du consentement prônée par la Charte et le RGPD.

3. La subsidiarité du consentement, une solution durable au traitement des données ?

Si l'approche collective du consentement ne représente pas une option réaliste pour franchir les défis issus de la pratique dans un environnement numérique en expansion, nous croyons qu'une reconsidération du poids du consentement vis-à-vis des autres bases de licéité pourrait en revanche constituer une solution viable. Bien qu'il n'existe aucune hiérarchie entre les six fondements énumérés à l'article 6, §1er, du RGPD[195], il est clair que le consentement a toujours été placé en tête des conditions de licéité[196], ne fût-ce que symboliquement. Notre propos revient donc à désacraliser le consentement et à lui reconnaître une place subsidiaire au bénéfice des autres bases de licéité que sont l'exécution d'un contrat, le respect d'une obligation légale, la sauvegarde d'intérêts vitaux, l'exécution d'une mission d'intérêt public et la poursuite d'un intérêt légitime par le responsable du traitement ou par un tiers[197].

La reconnaissance d'une subsidiarité du consentement présente l'avantage de ne pas nécessiter une modification du cadre législatif actuellement en vigueur. Nous pensons en effet qu'une interprétation plus souple du RGPD peut suffire pour consacrer un caractère subsidiaire au consentement et ainsi réduire les risques d'un usage abusif et inadéquat de ce dernier. Concrètement, il s'agirait d'encourager les responsables du traitement à fonder leurs opérations sur la base juridique la plus conforme aux finalités poursuivies et à ne recourir au consentement qu'en ultime recours, uniquement si aucun autre fondement ne permet de

---

[193] Nous soulignons.

[194] Article 8 de la Charte européenne des droits fondamentaux du 7 décembre 2000 (texte disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:12012P/TXT, site consulté le 22 avril 2020).

[195] Jean-Ferdinand PUYRAIMOND, *op. cit.*, p. 47.

[196] Yves POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.,* p. 14.

[197] Article 6, §1er, b) à f) du Règlement général sur la protection des données (RGPD).

justifier le traitement[198]. Dans le secteur public, où le recours au consentement est déjà peu fréquent, il serait ainsi souhaitable de continuer à privilégier les fondements d'obligation légale et d'exécution d'une mission d'intérêt public pour légitimer la plupart des traitements[199]. En revanche, dans le secteur privé, il conviendrait de recourir prioritairement à la nécessité du contrat à exécuter[200], puis, à défaut, à l'intérêt légitime supérieur du responsable du traitement[201]. Ce n'est qu'en dernier lieu que l'on trouvera dans le consentement la base juridique nécéssaire pour fonder tout traitement qui n'aurait pas pu être justifié par une autre base[202].

La mise en œuvre de la subsidiarité ne repose pas uniquement sur une érosion progressive du consentement mais elle implique parallèlement le besoin d'un réexamen du poids des autres bases de licéité énumérées à l'article 6, §1er, du RGPD. Ce nouvel équilibre auquel nous appelons devra impérativement prendre en compte la réalité technologique. Ainsi, pour ne prendre que l'exemple de l'intérêt légitime supérieur, celui-ci est sans aucun doute amené à évoluer pour s'adapter au contexte numérique dans lequel on l'invoque. Pour qu'un traitement

---

198 Dans son avis du 13 juillet 2011 sur la définition du consentement, le Groupe de travail de l'article 29 présente un exemple en ce sens dans le cadre particulier de l'achat d'une voiture. Il suggère ainsi que les données qui sont nécessaires à l'achat de la voiture soient traitées sur la base de l'exécution d'un contrat (article 6, §1er, b) du RGPD) tandis que le respect d'obligations légales justifierait le traitement des documents du véhicule (article 6, §1er, c) du RGPD). En outre, le responsable du traitement pourrait recourir à l'intérêt légitime pour les services de gestion des données de la clientèle (article 6, §1er, f) du RGPD). Enfin, le consentement pourrait quant à lui être utilisé pour légitimer le transfert des données à des tiers aux fins de leurs propres activités de commercialisation (article 6, §1er, a) du RGPD). (Voy. Groupe de travail de l'article 29 sur la définition du consentement, 01197/11/FR WP 187, adopté le 13 juillet 2011, p. 9. Document disponible sur https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp187_fr.pdf, site consulté le 22 avril 2020).

199 Informations recueillies le 7 avril 2020 auprès de Monsieur François GADISSEUR, délégué à la protection des données au sein du Parlement de Wallonie.

200 Parmi les fondements de licéité alternatifs au consentement, l'hypothèse de l'exécution d'un contrat devrait être préférée au consentement toutes les fois où ils sont mis en concurrence l'un et l'autre. Pour la plupart des contrats traditionnels où un client règle en monnaie, l'exécution d'une prestation implique le traitement de données telles que l'adresse de livraison, le nom du client, etc. Dans l'environnement numérique, l'exécution de contrats requiert également le traitement de données, celles-ci pouvant être assimilées à une contrepartie économique. Ainsi, par exemple, dès qu'un internaute créerait un compte en ligne, il faudrait y voir la conclusion d'un contrat qui autorise le traitement de données pour autant que celles-ci soient nécessaires à l'exécution dudit contrat. Dans ces cas, les demandes de consentement seraient donc à exclure (Emmanuel NETTER, *op. cit.*, pp. 171-172).

201 Notons que l'intérêt légitime a lui-aussi fait l'objet de critiques au motif qu'il installerait de l'insécurité juridique pour les personnes concernées. C'est ce qui pousse Jean-Ferdinand PUYRAIMOND à préférer le consentement à l'intérêt légitime pour justifier le traitement de données à caractère personnel. Ainsi, selon lui, « aussi critique que l'on puisse être vis-à-vis du fondement du consentement et même s'il est vrai que les personnes souvent ne lisent pas les conditions qu'elles acceptent en ligne, il n'en reste pas moins que le droit de retrait [du consentement] est une arme juridique efficace. Le fondement de l'intérêt légitime dépossède au contraire la personne concernée de sa maîtrise sur ses données et, sauf dans des cas comme le direct *marketing*, n'offre à la personne concernée qu'un droit d'opposition assez incertain et dont tant l'effectivité que l'efficacité peuvent laisser dubitatif » (Jean-Ferdinand PUYRAIMOND, *op. cit.*, p. 75). Nous tenons toutefois à préciser que la balance d'intérêts qui doit être réalisée entre les droits fondamentaux de la personne concernée et les intérêts légitimes du responsable du traitement est de nature à éviter un recours abusif à la base de licéité de l'intérêt légitime puisque seul un intérêt impérieux du responsable du traitement justifie une ingérence importante dans les intérêts de la personne concernée.

202 Pour un avis similaire, voy. Yves POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.,* p. 17.

soit licite sur la base d'intérêts légitimes, la Cour de justice a énoncé trois conditions cumulatives « à savoir, premièrement, la poursuite d'un intérêt légitime par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, deuxièmement, la nécessité du traitement des données à caractère personnel pour la réalisation de l'intérêt légitime poursuivi et, troisièmement, la condition que les droits et les libertés fondamentaux de la personne concernée par la protection des données ne prévalent pas »[203] sur l'intérêt légitime du responsable du traitement ou des tiers. Cette troisième condition fait l'objet d'une évaluation au cas par cas qui dépend notamment du contexte dans lequel les parties en cause sont placées[204]. À l'heure des technologies du *big data*, il est clair que la pondération des intérêts devra évoluer en conséquence, en prenant en compte d'une part, les nouveaux intérêts poursuivis par les responsables du traitement ainsi que, d'autre part, les risques croissants auxquels les personnes concernées s'exposent sur Internet.

En tant qu'organe indépendant de l'Union européenne doté de la personnalité juridique[205], nous sommes d'avis que le Comité européen de la protection des données est tout à fait capable de nourrir de futures réflexions nécessaires à la mise en œuvre d'une subsidiarité du consentement. Fort de sa compétence consultative, il pourrait ainsi conseiller la Commission « sur toute question relative à la protection des données à caractère personnel dans l'Union, y compris sur tout projet de modification du [RGPD] »[206]. Ce rôle consultatif peut également se matérialiser sous la forme de lignes directrices, de recommandations ou de guides de bonnes pratiques ayant pour objet une meilleure application du RGPD[207]. Outre cette compétence d'avis, il convient de signaler que le Comité est susceptible d'adopter des décisions contraignantes à l'égard des autorités nationales de contrôle en vue d'une bonne application du RGPD dans l'ensemble des États membres.

Nous pensons, par ailleurs, que la Commission européenne peut, de sa propre initiative ou sur la base des conseils du Comité européen de la protection des données, jouer un rôle actif afin d'atteindre le nouvel équilibre entre les différents fondements au traitement de données. Pour rappel, au cours des débats précédant l'adoption du RGPD, celle-ci avait déjà marqué son intention de renforcer la protection des données des utilisateurs d'Internet en généralisant l'exigence d'un consentement explicite. Cette option n'a pas été suivie et le caractère univoque du consentement lui a finalement été préféré[208]. Sans pour autant envisager l'élaboration d'une proposition législative, la Commission européenne pourrait, selon nous, suivre la voie de la subsidiarité du consentement en apportant certaines précisions au sein d'un avis. Bien que l'interprétation contraignante de la législation de l'Union européenne relève de la compétence

---

[203] C.J.U.E., 4 mai 2017, *arrêt Rigas Satiksme*, C-13/16, point 28.

[204] Voy. le considérant 47 du Règlement général sur la protection des données (RGPD).

[205] Article 68 du Règlement général sur la protection des données (RGPD).

[206] Article 70, §1er, b), du Règlement général sur la protection des données (RGPD).

[207] Romain ROBERT, « Le Comité européen de la protection des données : le garant d'un nouvel ordre ? » in Cécile DE TERWANGNE et Karen ROSIER (dirs.), *Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Larcier, 2018, p. 622.

[208] Cécile DE TERWANGNE et Karen ROSIER, *op. cit.*, p. 125.

exclusive de la Cour de justice[209], rien n'empêche à la Commission européenne d'initier quelques réflexions relatives à un nouvel équilibre entre les six bases de licéité fixées au sein du RGPD.

L'idée d'une subsidiarité du consentement est, nous le croyons, une option appropriée pour relever un certain nombre de défis issus de la pratique dans un environnement numérique. Toutefois, il faut bien se rendre compte qu'un tel raisonnement conduit à réserver le consentement aux traitements les plus difficilement justifiables étant donné que, par hypothèse, aucun autre fondement n'a pu être envisagé par voie de préférence. Autrement dit, la subsidiarité permet tout au plus de réduire les difficultés inhérentes au consentement sans réellement les faire disparaître. Il ne faut donc voir là qu'une solution transitoire qui ne remplace nullement le besoin de réévaluer en profondeur la place qu'occupe le consentement ainsi que les autres bases de licéité au sein du RGPD.

[209] Commission européenne, « Le RGPD : nouvelles opportunités, nouvelles obligations », brochure à destination des entreprises, 2019, p. 19. Document disponible sur https://ec.europa.eu/commission/sites/beta-political/files/gdpr2019-business_brochure-fr-v04_web.pdf, site consulté le 28 avril 2020.

CONCLUSION

En tant que représentation la plus évidente du droit à l'autodétermination informationnelle, le consentement est considéré comme l'un des piliers essentiels du droit européen de la protection des données. Avec l'adoption du RGPD, le législateur européen a renforcé les exigences de qualité du consentement en réaction aux situations de plus en plus fréquentes dans lesquelles un consentement de mauvaise qualité servait de fondement au traitement de données à caractère personnel. Le cumul d'autant de qualités est-il toutefois suffisant pour assurer à lui seul une protection efficace et effective des personnes concernées dont les données ne cessent d'être toujours plus convoitées ? Devant la réalité des consentements exprimés sur Internet, dont la plupart sont creux et vides de signification, force est de constater que les bonnes intentions du législateur européen sont vouées à demeurer des vœux pieux.

Ce constat préoccupant a toutes les raisons de nourrir d'importantes réflexions doctrinales lorsque l'on prend conscience des nombreux dangers qui accompagnent l'inexorable essor du numérique. Pour que nos données ne soient pas aspirées par le phénomène des *big data* et que nous gardions sur elles un contrôle entier, il est urgent de penser dès à présent à des solutions réalistes qui concilient les innovations technologiques et la protection des données. Bien loin d'être une solution infaillible, la subsidiarité représente sans doute une option qui permettrait de réduire les difficultés inhérentes au consentement, du moins temporairement. En tout cas, quelle que soit la voie dans laquelle évoluera la notion de consentement, celle-ci devra non seulement tenir compte des signaux issus de la pratique, mais aussi des enjeux de la société numérique pour assurer durablement l'efficacité du droit de la protection des données au sein de l'Union européenne.

BIBLIOGRAPHIE

1. Sources doctrinales

1.1. Monographies

BEELEN, Axel, *Guide pratique du RGPD - Fiches de guidance,* Bruxelles, Bruylant, 2018, 370 pages.

BENSOUSSAN, Alain et BENSOUSSAN, Jérémy, *IA, robots et droit*, Bruxelles, Bruylant, 2019, 652 pages.

BENSOUSSAN, Alain, *La protection des données personnelles de A à Z*, Bruxelles, Bruylant, 2017, 272 pages.

BENSOUSSAN, Alain, *Règlement européen sur la protection des données, textes, commentaires et orientations pratiques*, Bruxelles, Larcier, 2016, 708 pages.

BETKIER, Marcin, *Privacy Online, Law and the Effective Regulation of Online Services,* Cambridge, Intersentia, 2019, 283 pages.

BYGRAVE, Lee et WIESE SCHARTUM, Dag « Consent, Proportionality and Collective Power », *in* GUTWIRTH, Serge, POULLET, Yves, DE HERT, Paul, DE TERWANGNE, Cécile et NOUWT, Sjaak (éds.), *Reinventing Data Protection ?*, Heidelberg, Springer, 2009, 372 pages.

CARNEROLI, Sandrine, *Marketing et internet*, Bruxelles, Larcier, 2011, 134 pages.

COHEN, Julie, « Between Truth and Power », *in* Mireille HILDEBRANDT et Bibi VAN DEN BERG (eds.), *Information, Freedom and Property,* Routledge, Abingdon, 2016, 202 pages.

COTON, Fanny et LIMBRÉE, Pauline, « Les données, des armes de déduction massive (données massives, recherche scientifique, profilage et décision automatisée à l'ère du Règlement Général sur la Protection des Données) » *in* CASSART, Alexandre (coord.), *Le droit des MachinTech (FinTech, LegalTech, MedTech...)*, Bruxelles, Larcier, 2018, 230 pages.

DANNEELS, Paul, « Fundamenten voor een AI gedreven notariaat » in *Tradition in motion*, Gent, Larcier, 2019, 321 pages.

DE TERWANGNE, Cécile et VAN ENIS, Quentin, *L'Europe des droits de l'homme à l'heure d'Internet,* Bruxelles, Bruylant, 2019, 717 pages.

DE TERWANGNE, Cécile, DEGRAVE, Elise, DELFORGE, Antoine, et GÉRARD, Loïck, *La protection des données à caractère personnel en Belgique*, Bruxelles, Politeia, 2019, 189 pages.

DE TERWANGNE, Cécile et ROSIER, Karen, *Le règlement général sur la protection des données (RGPD/GDPR) - Analyse approfondie*, Bruxelles, Larcier, 2018, 928 pages.

DE TERWANGNE, Cécile et VAN GYSEGHEM, Jean-Marc, *Vie privée et données à caractère personnel*, Bruxelles, Politeia, 2013, pag. mult.

DEBET, Anne, MASSOT, Jean et METALLINOS Nathalie, *Informatique et libertés - la protection des données à caractère personnel en droit français et européen*, Issy-les-Moulineaux, Lextenso, 2015, 1288 pages.

DELFORGE, Antoine et GERARD, Loïck, « Notre vie privée est-elle réellement mise en danger par les robots ? Étude des risques et analyse des solutions apportées par le GDPR », *in* JACQUEMIN, Hervé et DE STREEL, Alexandre (coord.), *L'intelligence artificielle et le droit*, Bruxelles, Larcier, 2017, 482 pages.

DESGENS-PASANAU, Guillaume, *La protection des données personnelles - Le RGPD et la loi française du 20 juin 2018*, 4e éd., Paris, LexisNexis, 2019, 345 pages.

DOCQUIR, Benjamin, *Répertoire pratique du droit belge - Législation, Doctrine, Jurisprudence - Droit du numérique,* Bruxelles, Larcier, 2018, 678 pages.

DOCQUIR, Benjamin, *Vers un droit européen de la protection des données ?*, Bruxelles, Larcier, 2017, 175 pages.

DOCQUIR, Benjamin « Consentement et intérêt légitime dans le secteur privé », *in* RAGHENO, Nathalie (coord.), *Data Protection & Privacy. Le GDPR dans la pratique/De GDPR in de praktijk,* Limal, Anthemis, 2017, 230 pages.

DUMORTIER, Jos et ROBBEN, Frank, *Persoonsgegevens en privacybescherming, Commentaar op de wet tot bescherming van de persoonlijke levenssfeer*, Bruges, die Keure, 1995, 348 pages.

HENRY, Patrick, « Fiona, Tina et le monde d'hier » *in* DE CODT, Jean, DECONINCK, Beatrijs, THIJS, Dirk et VAN DROOGHENBROECK, Jean-François (dirs.), *Le Code judiciaire a 50 ans. Et après ? / 50 jaar Gerechtelijk Wetboek. Wat nu ?*, Bruxelles, Larcier, 2018, 809 pages.

JACQUEMIN, Hervé et NIHOUL, Marc, *Vulnérabilités et droits dans l'environnement numérique*, Bruxelles, Larcier, 2018, 626 pages.

KOSTA, Eleni, *Consent in European Data Protection Law,* Leiden, Martinus Nijhoff, 2013, 442 pages.

KUNER, Christopher, *European Data Privacy Law and Online Business,* Oxford, Oxford University Press, 2003, 322 pages.

LELEU, Yves-Henri, *Droit des personnes et des familles*, 3e éd., Bruxelles, Larcier, 2016, 904 pages.

LÉONARD, Thierry, « Yves, si tu exploitais tes données », *in* DEGRAVE, Élise, DE TERWANGNE, Cécile, DUSOLLIER, Séverine et QUECK, Robert (dirs.), *Law, Norms and Freedoms in Cyberspace - Droit, normes et libertés dans le cybermonde - Liber Amicorum Yves POULLET*, Bruxelles, Larcier, 2018, 800 pages.

LOBET-MARIS, Claire « Du fétichisme de la donnée personnelle. Relecture politique et critique de la vie privée » *in* DEGRAVE, Élise, DE TERWANGNE, Cécile, DUSOLLIER, Séverine et QUECK, Robert (dirs.), *Law, Norms and Freedoms in Cyberspace - Droit, normes et libertés dans le cybermonde - Liber Amicorum Yves POULLET*, Bruxelles, Larcier, 2018, 800 pages.

POULLET, Yves, *La vie privée à l'heure de la société du numérique*, Bruxelles, Larcier, 2019, 190 pages.

ROBERT, Romain, « Le Comité européen de la protection des données : le garant d'un nouvel ordre ? » *in* DE TERWANGNE, Cécile et ROSIER, Karen (dirs.), *Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Larcier, 2018, 928 pages.

ROUVROY, Antoinette, « Homo juridicus est-il soluble dans les données ? » *in* DEGRAVE, Élise, DE TERWANGNE, Cécile, DUSOLLIER, Séverine et QUECK, Robert (dirs.), *Law, Norms and Freedoms in Cyberspace - Droit, normes et libertés dans le cybermonde - Liber Amicorum Yves POULLET*, Bruxelles, Larcier, 2018, 800 pages.

TAMBOU, Olivia, *Manuel de droit européen de la protection des données à caractère personnel*, Bruxelles, Bruylant, 2020, 486 pages.

VAN DEN BRANDEN, Adrien, *Les robots à l'assaut de la justice - L'intelligence artificielle au service des justiciables,* Bruxelles, Bruylant, 2019, 162 pages.

1.2. Revues périodiques

BOULANGER, Marie-Hélène, DE TERWANGNE, Cécile, LEONARD, Thierry, LOUVEAUX, Sophie, MOREAU, Damien et POULLET Yves, « La protection des données à caractère personnel en droit communautaire », *J.T. dr. eur.*, 1997, pp. 121-127.

CHANCERELLE, Liane, « La lutte contre les discriminations en Europe à l'ère de l'intelligence artificielle et du big data », *J.D.J.*, 2019/1, pp. 25-37.

COHEN, Julie, « Privacy, Ideology and Technology », *The Georgetown Law Journal*, 2001/89, pp. 2029-2045.

JANSSENS, Karel et NUYTTEN, Marion, « De Algemene Verordening Persoonsgegevens : van theorie naar praktijk », *R.D.C.-T.B.H.*, 2018/5, pp. 401-435.

LÉONARD, THIERRY et POULLET, Yves, « La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la Directive 95/46/CE du 24 octobre 1995 », *J.T.*, 1999, pp. 377-396.

MAIRLOT, Miguel, « Big Data et vie privée : mariage possible ? », *D.B.F.-B.F.R.*, 2015/6, pp. 446-451.

MARTIAL-BRAZ, Nathalie, « Les nouveaux droits des personnes concernées », *R.A.E.-L.E.A.*, 2018/1, pp. 7-17.

MEYER, Julie, DANTAN, Estelle, LANGE, Fanny, GOURZONES, Célia et SADAKA, Elsa, « La C.J.U.E. rejette la présomption de consentement au placement des *cookies* », *La revue des droits de l'homme* [en ligne], 2020, pp. 1-6.

MICHEL, Alejandra, « Le traçage comportemental des internautes sur les réseaux sociaux : l'affaire des *"cookies Facebook"*, véritable saga judiciaire ? », *R.D.T.I.*, 2019/1, pp. 72-92.

MOINY, Jean-Philippe, « Facebook au regard des règles européennes concernant la protection des données », *R.E.D.C.*, 2010/2, pp. 235-271.

MONT, Julie, « R.G.P.D. : quelles nouvelles règles pour les enfants sur Facebook ? », *R.D.T.I.*, 2019/75, pp. 5-25.

NETTER, Emmanuel, « Sanction à 50 millions d'euros : au-delà de Google, la CNIL s'attaque aux politiques de confidentialité obscures et aux consentements creux », *Dalloz IP/IT*, 2019, pp. 165-172.

NOTO LA DIEGA, Guido « Some Considerations on Intelligent Online behavioural Advertising », *R.D.T.I.*, 2017/66-67, pp. 53-90.

POULLET, Yves, « Consentement et RGPD : des zones d'ombre ! », *D.C.C.R.*, 2019/1-2, pp. 3-37.

PURTOVA, Nadezhda, « Do Property rights in personal data make sense after the big data turn ? », *Journal of Law and Economic Regulation,* 2017/10, pp. 64-78.

PUYRAIMOND, Jean-Ferdinand, « L'intérêt légitime du responsable du traitement dans le RGPD : *in causa venenum ?* », *DCCR,* 2019/122-123, pp. 39-77.

REINSEL, David, GANTZ, John et RYDNING, John, « Data Age 2025 : The Evolution of Data to Life-Critical - Don't Focus on Big Data ; Focus on the Data That's Big », *IDC*, 2017, pp. 1-25.

ROBERT, Romain et PONSART, Chloé, « Le règlement européen de protection des données personnelles », *J.T.*, 2018/20, pp. 421-438.

ROSIER, Karen, FIEVET, Coline, GERARD, Loïck, VANRECK, Odile, MICHEL, Alejandra, MONT, Julie, KNOCKAERT, Manon, GILLARD, Noémie et TOMBAL, Thomas, « Droit au respect de la vie privée et à la protection des données en lien avec les technologies de l'information - Chronique de jurisprudence 2015-2017 », *R.D.T.I.*, 2017/3-4, pp. 94-163.

ROSIER, Karen, « Les réseaux sociaux et les jeunes : la Commission européenne exhorte à une protection renforcée de leur vie privée », *B.J.S.*, 2011/460, p. 14.

RUE, Guillaume, « Le placement de cookies requiert le consentement actif des internautes », *B.J.S.*, 2019/639, p. 11.

RUE, Guillaume, « L'autorité de protection des données impose une amende pour des *cookies* non conformes », *B.J.S.*, 2020/643, p. 11.

SCHERMER, Bart Willem, CUSTERS, Bart et VAN DER HOF, Simone, « The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection », *Ethics & Information Technology*, 2014/16, pp. 171-182.

SOLOVE, Daniel, « Introduction : Privacy Self-Management and the Consent Dilemma », *Harvard Law Review*, 2013/126, pp. 1880-1903.

VAN GYSEGHEM, Jean-Marc, DE TERWANGNE, Cécile, HERVEG, Jean et GAYREL, Claire, « La protection des données à caractère personnel en droit européen - Data Protection in European Law », *JEDH*, 2014/1, pp. 54-87.

VAN OVERSTRAETEN, Marc et DEPRÉ, Sébastien, « Le traitement automatisé des données à caractère personnel et le droit au respect de la vie privée en Belgique », *Rev. trim. dr. h.*, 54/2003, pp. 665-701.

2. Sources jurisprudentielles

2.1. Tribunal de première instance (Belgique)

Civ. Bruxelles (24e ch. N), 16 février 2018, R.G. n°2016/153/A, *R.D.T.I.*, 2019/1, pp. 71 et s.

2.2. Cour de justice de l'Union européenne

C.J.U.E., 1er octobre 2019, *arrêt Planet49*, C-673/17.

C.J.U.E., 4 mai 2017, *arrêt Rigas Satiksme*, C-13/16, point 28.

C.J.U.E., 24 novembre 2011, *arrêt ASNEF et FECEMD c. Administracion del Estado*, C-468/10 et C-469/10.

C.J.U.E., 2 décembre 2010, *arrêt Ker-Optika*, C-108/09.

C.J.C.E., 20 mai 2003, *arrêts Rechnungshof c. Österreichischer Rundfunk e.a.*, C−465/00, C−138/01 et C−139/01.

3. Sources Internet

Autorité de protection des données, chambre contentieuse, décision quant au fond 12/2019, 17 décembre 2019. Document disponible sur https://www.autoriteprotectiondonnees.be/decisions-de-la-chambre-contentieuse.

Autorité de protection des données, communiqué de presse du 13 février 2018. Document disponible sur https://www.autoriteprotectiondonnees.be/news/rgpd-la-limite-dage-de-13-ans-correspond-a-la-pratique-numerique.

Autorité de protection des données, « Le nouveau règlement opère un changement important par rapport à la Directive 95/46 et prône le principe de l'*accountability* (ou de responsabilité) ».

Document disponible sur https://www.autoriteprotectiondonnees.be/principe-de-responsabilite-accountability.

Charte européenne des droits fondamentaux du 7 décembre 2000. Document disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:12012P/TXT.

Commission européenne, « Le RGPD : nouvelles opportunités, nouvelles obligations », brochure à destination des entreprises, 2019. Document disponible sur https://ec.europa.eu/commission/sites/beta-political/files/gdpr2019-business_brochure-fr-v04_web.pdf.

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 28 janvier 1981. Document disponible sur https://www.coe.int.

Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679,* 17/FR WP 259, révisées et adoptées le 10 avril 2018. Document disponible sur https://www.cnil.fr/sites/default/files/atoms/files/ldconsentement_wp259_rev_0.1_fr.pdf.

Groupe de travail de l'article 29 lignes directrices sur *les décisions individuelles automatisées et le profilage au titre du Règlement 2016/679,* 17/EN WP 251, révisées et adoptées le 6 février 2018. Document disponible sur https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

Groupe de travail de l'article 29, *Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE,* 844/14/FR WP 217, adopté le 9 avril 2014. Document disponible sur https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf.

Groupe de travail de l'article 29 sur la définition du consentement, 01197/11/FR WP 187, adopté le 13 juillet 2011. Document disponible sur https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp187_fr.pdf.

Information Commissioner's Office (UK), « Consultation : GDPR consent guidance », 31 mars 2017, pp. 33-34. Document disponible sur https://iapp.org/media/pdf/resource_center/ICO-gdpr-consent-guidance.pdf.

Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données à caractère personnel, 23 septembre 1980. Document disponible sur https://www.oecd.org.

Microsoft, « Voice report - From answers to action : customer adoption of voice technology and digital assistants », 2019, pp. 8 et s. Document disponible sur https://advertiseonbing-blob.azureedge.net/blob/bingads/media/insight/whitepapers/2019/04%20apr/voice-report/bingads_2019voicereport.pdf.

Norme ISO/IEC 27701:2019, « Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices ». Résumé de la norme disponible sur https://www.iso.org/fr/standard/71670.html.

Norme ISO/IEC 27001 « management de la sécurité de l'information ». Résumé de la norme disponible sur https://www.iso.org/fr/isoiec-27001-information-security.html.

Norme ISO/IEC 2382:2015, « Technologies de l'information - Vocabulaire », norme disponible sur https://www.iso.org/fr/standard/63598.html.

PECB, « ISO/IEC 27701 - Système de management de la protection de la vie privée », analyse descriptive de l'organisme de certification. Document disponible sur https://pecb.com/fr/education-and-certification-for-individuals/iso-iec-27701.

Principes directeurs des Nations Unies pour la règlementation des fichiers personnels informatisés, 14 décembre 1990. Document disponible sur https://www.un.org.

Rapport de l'OPECST, « Pour une intelligence artificielle maîtrisée, utile et démystifiée », t. I, enregistré à la présidence de l'Assemblée nationale et du Séant le 15 mars 2017. Document disponible sur http://www.senat.fr/rap/r16-464-1/r16-464-11.pdf.

Rapport explicatif de la version modernisée de la Convention n°108 du Conseil de l'Europe, adopté le 18 mai 2018, p. 22. Document disponible sur https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726.

REINSEL, David, GANTZ, John et RYDNING, John, « Data Age 2025 : The Evolution of Data to Life-Critical - Don't Focus on Big Data ; Focus on the Data That's Big », IDC, 2017. Document disponible sur https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/workforce/Seagate-WP-DataAge2025-March-2017.pdf.

Traité sur l'Union européenne. Document disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:12012P/TXT.

Université de Gand, *« Status quo regarding the child's article 8 GDPR age of consent for data processing across the EU »*. Document disponible sur https://www.betterinternetforkids.eu/en_US/web/portal/practice/awareness/detail?articleId=3017751.

4. Travaux parlementaires, rapports et lignes directrices

4.1. Travaux parlementaires belges

Projet de loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil 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, *Doc.*, Ch., 1997-1998, n°1566/1, p. 31.

4.2. Lignes directrices et avis du Groupe de travail de l'article 29

Groupe de travail de l'article 29 sur la protection des données, *Lignes directrices sur le consentement au sens du Règlement 2016/679,* 17/FR WP 259, révisées et adoptées le 10 avril 2018, pp. 1-36.

Groupe de travail de l'article 29 sur la protection des données, *lignes directrices sur les décisions individuelles automatisées et le profilage au titre du Règlement 2016/679,* 17/EN WP 251, révisées et adoptées le 6 février 2018, pp. 1-37.

Groupe de travail de l'article 29 sur la protection des données, *Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE,* 844/14/FR WP 217, adopté le 9 avril 2014, pp. 1-78.

Groupe de travail de l'article 29 sur la définition du consentement, 01197/11/FR WP 187, adopté le 13 juillet 2011, pp. 1-43.

4.3. Rapport du Comité LIBE du Parlement européen

Comité LIBE du Parlement européen du 22 novembre 2013 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) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Rapporteur Jan Philipp ALBRECHT, Exposé des motifs.