UCLouvain

Faculté de droit et de criminologie

Le traitement des données à caractère personnel opéré par Facebook à des fins de profilage publicitaire au regard du Règlement Général sur la Protection des Données

Les activités de Facebook peuvent-elles être conformes aux exigences du nouveau règlement européen ?

Auteur : Elisabeth MANS
Promoteur : Alexandre CRUQUENAIRE
Année académique 2018-2019
Master en Droit - Finalité spécialisée : Justice civile et pénale

Plagiat et erreur méthodologique grave

Le plagiat, fût-il de texte non soumis à droit d'auteur, entraîne l'application de la section 7 des articles 87 à 90 du règlement général des études et des examens.

Le plagiat consiste à utiliser des idées, un texte ou une œuvre, même partiellement, sans en mentionner précisément le nom de l'auteur et la source au moment et à l'endroit exact de chaque utilisation*.

En outre, la reproduction littérale de passages d'une œuvre sans les placer entre guillemets, quand bien même l'auteur et la source de cette œuvre seraient mentionnés, constitue une erreur méthodologique grave pouvant entraîner l'échec.

* A ce sujet, voy. notamment **http://www.uclouvain.be/plagiat**.

REMERCIEMENTS

Je tiens tout d'abord à remercier mon promoteur, Monsieur Alexandre Cruquenaire, pour la confiance qu'il m'a accordée dans le choix de ce sujet de mémoire. Il m'a offert l'opportunité de traiter une problématique qui me tient réellement à cœur et a cru en ma capacité d'y apporter l'angle de vue juridique nécessaire à sa compréhension profonde.

Je voudrais ensuite exprimer ma plus sincère reconnaissance envers mes parents, qui ont passé 22 ans à m'instruire, à m'éduquer et à m'apprendre, entre beaucoup d'autres choses, comment utiliser intelligemment l'outil merveilleux mais dangereux qu'est Internet. Et plus particulièrement durant les mois qui viennent de s'écouler, pour la patience dont ils ont fait preuve, pour leurs nombreuses relectures et surtout pour leurs conseils avisés dans le cadre de la rédaction de mon mémoire.

Enfin, j'aimerais adresser un merci tout particulier aux amis qui m'ont entourée sans relâche le long du chemin qu'a été cette écriture. Parce que la plus belle leçon que j'ai apprise au cours de mon parcours universitaire, c'est que tout accomplissement perdrait de sa saveur et de sa valeur s'il ne se partageait pas avec ceux qui nous accompagnent dans nos moments de doute, nos rires et nos espoirs.

TABLE DES MATIÈRES

Introduction

Description du contexte

Dès lors que n'importe quel individu connecte l'un de ses appareils à Internet ou même à un quelconque outil de localisation, ses faits et gestes (ainsi que ceux de son entourage) sont répertoriés, analysés et utilisés à des fins diverses et variées. Cela a tendance à donner aux utilisateurs d'Internet l'impression d'être tracés[1]. Pourtant, même s'ils sont de plus en plus conscients que toutes les données qu'ils exposent à la vue de l'œil inquisiteur d'Internet seront stockées et mises à profit, très rares sont ceux qui comprennent pourquoi et comment. Il est presque impossible de connaître toutes les ficelles des mécanismes qui se cachent derrière la récolte de ces données et l'utilisation qui en est faite. Par ailleurs, les règles applicables à la protection des données à caractère personnel n'ont jamais vraiment été connues du grand public.

Le 25 mai 2018 entrait en application le Règlement Général sur la Protection des Données (RGPD, ou G.D.P.R. en anglais)[2]. Cet évènement juridique a fait énormément de bruit tant dans l'Union Européenne que dans le reste du monde[3], et les réactions ont été différentes selon les intérêts des principaux intéressés. Pour les individus, cela a paru être une avancée de la protection des données à caractère personnel et de la vie privée sur l'invasion du numérique, mais du point de vue des organisations et entreprises, le RGPD a de suite été perçu comme une contrainte.

En ce qui concerne les individus, il semble pourtant évident qu'ils n'ont été que très peu informés de ses implications réelles. Il est regrettable que l'entrée en application de cette nouvelle réglementation n'ait pas été l'occasion de générer une sensibilisation plus approfondie de la population quant à l'importance que représentent les données personnelles et les droits dont les individus disposent à cet égard[4]. La mise en application de RGPD a donné l'impression assez

---

[1] J.-F. PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *D.C.C.R.*, 2019/1-2, n°122-123, p. 41.

[2] Règlement (UE) n° 679/2016 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119, 4 mai 2016, p. 001, art. 99, §2.

[3] N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *R.D.C.-T.B.H.*, 2019/1, p. 53.

[4] DOUCET B., « Avez-vous lu les conditions générales ? "GDPR, une occasion manquée ?"» *in Louvains mars-avril-mai 2018*, (article en ligne disponible sur https://uclouvain.be/fr/decouvrir/louvains/avez-vous-lu-les-conditions-generales.html consulté le 12 juillet).

généralisée que le problème était résolu, et que les données personnelles étaient dès lors saines et sauves. Or c'est loin d'être le cas. Premièrement parce qu'en substance le RGPD n'apporte que très peu de modifications majeures à la législation qui était d'application jusqu'alors[5]. Deuxièmement parce que la plupart des modifications substantielles qui sont survenues avec la mise en application de RGPD (notamment le droit à la portabilité des données[6]) nécessitent une participation active des individus pour qu'elles aient l'occasion d'avoir une réelle efficacité[7]. Il n'en reste pas moins que le rôle joué par les contrôles des Autorités de Protection des Données (APD) nationales dans la pratique est capital. En Belgique par exemple, la CPVP, ou Commission de Protection de la Vie Privée a été transformée en APD par la loi du 3 décembre 2017, entrée en vigueur le 10 janvier 2018[8] et s'est vu octroyer à cette occasion des pouvoirs supplémentaires lui permettant de faire appliquer le RGPD et les sanctions y afférentes[9].

En ce qui concerne les organisations et entreprises, la tâche que représente la mise en conformité au RGPD est loin d'être simple[10], en particulier du fait du contrôle des Autorités précitées. Même si le seuil d'exigence des législations européennes précédentes était presque aussi élevé, les amendes applicables ayant pris une ampleur considérable et les contrôles étant renforcés, la nécessité de se plier à la norme est désormais bien réelle[11].

On peut donc s'interroger sur la raison pour laquelle les entreprises continuent à exploiter tant de données à caractère personnel (dites "données personnelles"), dans la mesure où cela représente désormais un tel risque financier. La réponse est à la fois évidente et complexe. Dans le cas de sociétés prodiguant des biens et services aux consommateurs, un nombre minimal de données personnelles est pour le moins nécessaire afin de les identifier sans ambiguïté. Mais la constitution et l'accroissement d'un fichier client fait très vite apparaître de nouvelles opportunités de

---

[5] Directive (CE) n° 46/1995 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, p. 031.

[6] C. PONSART et R. ROBERT, « Le règlement européen de protection des données personnelles », *J.T.*, 2018, p. 428.

[7] F. COTON et P. LIMBREE, « 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 Le droit des MachinTech (FinTech, LegalTech, MedTech,...)*, Bruxelles, Larcier, 2018, p. 78.

[8] Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018, p. 989.

[9] D. VAN BRIEL et A. VAN DE MEULEBROUCKE, *Commission vie privée devient Autorité de Protection des Données*, le 10 janvier 2018 (article en ligne disponible sur https://www.eubelius.com/fr/nouvelles/commission-vie-privee-devient-autorite-de-protection-des-donnees, dernière consultation le 06 août 2019).

[10] T. VAN CANNEYT, « The general data protection regulation : 10 things company lawyers should know », *C.J.*, 2016/1, p. 11.

[11] A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *R.D.T.I.,* 2018/1, n° 70, p. 28.

bénéfices[12]. C'est là que la problématique devient complexe. Des données de tous types concernant les individus sont amassées et détournées à des fins commerciales et économiques[13]. L'aspect patrimonial des données personnelles pèse donc plus dans la balance que les efforts à fournir pour se mettre en conformité… ou pour assumer les conséquences d'une mauvaise utilisation des données personnelles.

L'illustration la plus parlante de dérive en la matière est le profilage publicitaire. Qu'il s'agisse de prospectus dans les boîtes aux lettres, de courriers électroniques dans les boites mails ou d'encarts publicitaires sur les sites consultés, tout porte à croire que les entreprises ont une idée de plus en plus précise de ce qui intéresse les individus. Au-delà des "spams" classiques dont ceux-ci ont vite fait de se débarrasser, il semble évident que souvent les marques et les produits qui leur sont proposés reflètent leurs goûts, voire leur personnalité. C'est par un processus complexe de traitement, d'échange et de marchandage de leurs données personnelles – à leur insu – que ce "ciblage" étonnamment précis est rendu possible[14].

Il est évident que certaines entreprises ont mis cette pratique en œuvre et l'ont utilisée à son paroxysme, tout particulièrement Google et Facebook[15]. Grâce à cette pratique d'exploitation des données personnelles, ces géants d'Internet sont à même d'offrir leurs services sans les rendre payants[16]. Une formule imagée permet de comprendre le subterfuge : « *Si c'est gratuit, vous êtes le produit* »[17]. Vous, en ce qu'il y a de plus privé, à savoir vos données personnelles. Expliqué de manière vulgarisée par une vidéo de l'agence de communication Adesias en 2013[18], ce slogan a été recyclé à de nombreuses reprises. Il a plus récemment été utilisé par Tim Cook, dirigeant d'Apple, dans une critique du « *modèle économique de Facebook, centré sur la monétisation des données personnelles* »[19], dans le cadre des récentes accusations ayant accablé de toutes parts le dirigeant de ce réseau social, Marc Zuckerberg. Nous ne nous attarderons pas sur le scandale médiatique généré

---

[12] Y. POULLET, « Consentement et RGPD : des zones d'ombre ! », *D.C.C.R.*, 2019/1-2, n° 122-123, p.18.
[13] J.-F. PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *op. cit.*, p. 40.
[14] *Ibid*., p. 41.
[15] A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *in Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, p. 282.
[16] J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *R.E.D.C.*, 2010/2, p. 240.
[17] *Si c'est gratuit, vous êtes le produit*, Adesias, 2013 (article en ligne disponible sur https://adesias.fr/animation/adesias-si-c-est-gratuit-vous-êtes-le-produit/-u658, dernière consultation le 06 août 2019).
[18] *Ibid.*
[19] P. MABILLE, *Si c'est gratuit, c'est que vous êtes le produi*t, La Tribune, le 10 avril 2018 (article en ligne disponible sur https://www.latribune.fr/opinions/editos/si-c-est-gratuit-c-est-que-vous-etes-le-produit-774672.html, dernière consultation le 06 août 2019).

par les échanges violents qui s'en sont ensuivis entre ces deux concurrents. Nous préciserons toutefois que toute l'ironie de la situation repose dans le fait que Google, Amazon, Facebook et Apple, souvent repris sous l'acronyme "GAFA"[20], sont tous plus ou moins logés à la même enseigne en ce qui concerne la manière dont ils usent des données personnelles de leurs utilisateurs. Celles-ci sont rassemblées de diverses manières, échangées (entre grandes et petites entreprises) et représentent aujourd'hui un potentiel économique incontournable. C'est une des seules manières permettant à Facebook de fonctionner et de survivre. Pour pouvoir continuer à proposer du contenu et une plateforme gratuitement, il est nécessaire d'avoir une source de revenus. Les données personnelles et leur utilisation, plus particulièrement via le profilage publicitaire[21], assurent de rassembler suffisamment d'argent pour faire tourner le réseau social, rémunérer les employés de l'entreprise et couvrir le prix des infrastructures. Mais surtout pour générer une quantité astronomique de bénéfices. Ceux de Facebook dépassent les vingt-deux milliards chaque année[22]. Mais jusqu'où les pratiques permettant la monétisation des données sont-elles légitimes et légales[23] ?

Présentation du sujet d'étude

Le sujet est vaste, et les manières de l'aborder le sont tout autant. C'est pourquoi il est nécessaire de délimiter l'angle de vue selon lequel nous traiterons de cette problématique. Tout d'abord d'un point de vue juridique, la mise en application récente du RGPD est l'occasion parfaite pour analyser ce qui est exigé par la norme en matière de protection des données, qu'il s'agisse des grands principes repris par ce nouveau règlement dans les anciennes législations ou des innovations amenées lors de sa conception.

Néanmoins, les discussions ont été longues et les amendements nombreux, et le texte en découlant est si long et complexe qu'il serait impossible de l'analyser dans son ensemble et dans ses

---

[20] G. KOENIG, « Introduction », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles*, (Sous la direction de LÉGER L.), janvier 2018 (disponible sur https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf, dernière consultation le 06 août 2019), p. 13.

[21] *Ibid.*, p. 14.

[22] *Amende record pour Facebook : "Une centralisation des données personnelles sans équivalent à l'échelle de la planète"*, Franceinfo, le 13 juillet 2019 (article en ligne disponible sur https://www.francetvinfo.fr/Internet/reseaux-sociaux/facebook/amende-record-pour-facebook-une-centralisation-des-donnees-personnelles-sans-equivalent-a-l-echelle-de-la-planete_3534451.html, dernière consultation le 06 août 2019).

[23] « Résumé », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles*, (Sous la direction de LÉGER L.), janvier 2018 (disponible sur https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf, dernière consultation le 06 août 2019), p.8.

moindres détails dans le cadre de ce travail. L'originalité de cette étude réside justement dans l'approche choisie pour aborder le sujet, qui consiste à partir non pas de l'individu et des possibilités qui lui sont offertes pour protéger sa vie privée, mais d'une entreprise et de l'état de la conformité de ses actions. Comme nous l'avons évoqué plus tôt, une sensibilisation réelle des masses n'a pas été mise en place, et nous sommes conscients de la difficulté que représente cette tâche. Malgré les armes procurées et mises en évidence par la nouvelle réglementation, et les quelques poursuites déjà engagées par des individus, par des APD ou par des associations de protection des consommateurs, l'utilisateur moyen n'est pas toujours en mesure de faire valoir ses droits, même lorsqu'il dispose d'une information suffisante[24]. C'est pourquoi nous préférons partir de la source du problème - ou du moins d'une de ses sources.

Nous estimons qu'il est intéressant de se concentrer sur le cas de Facebook, au vu des nombreuses accusations dont le réseau social a dernièrement fait l'objet. Étant donné qu'il est extrêmement compliqué de savoir ce qu'il se passe réellement de l'autre côté des interfaces que nous connaissons si bien (et qui nous connaissent d'autant plus), ces accusations, les procédures qui en ont découlé et les récentes déclarations de Mark Zuckerberg représentent une opportunité considérable de mieux comprendre les pratiques sur lesquelles reposent le fonctionnement et la pérennité de Facebook. Même s'il est important de rester critique face aux informations dont nous disposons actuellement et de faire la part des choses, mettre à profit ces données nous permet de mieux comprendre comment il met nos propres données à profit. Principalement via la pratique du profilage publicitaire, sur laquelle nous nous concentrerons plus particulièrement puisqu'il s'agit d'un élément central et représentatif de cet enjeu.

Cette étude, qui portera donc sur le "traitement des données personnelles opéré par et via Facebook à des fins de profilage publicitaire au regard du Règlement Général sur la Protection des Données", sera divisée en quatre chapitres. Le premier répondra à la question incontournable de l'étendue de l'impact du RGPD sur Facebook, au travers de l'étude du champ d'application de cette réglementation. Le deuxième sera dédié à une définition du profilage publicitaire, à l'étude approfondie de ce processus complexe, ainsi que de la manière dont Facebook en use. Le troisième chapitre traitera du comportement recommandé par le RGPD en matière de protection des données.

---

[24] C. FRATI, *Le RGPD a une génération de retard,* interview de Cyril PIERRE-BEAUSSE, Paperjam, le 22 mars 2018 (article en ligne disponible sur http://paperjam.lu/news/le-rgpd-a-une-generation-de-retard, dernière consultation le 06 août 2019).

Le quatrième et dernier chapitre sera plus concis et aura pour objectif d'ouvrir une réflexion plus approfondie sur l'utilité du RGPD et sur le comportement adopté par Facebook actuellement, d'adopter un œil critique face à la pertinence du règlement et d'évaluer les solutions alternatives proposées.

Chapitre 1 : L'applicabilité du RGPD aux activités de Facebook

L'intervention du RGPD dans le paysage législatif européen est certes un évènement significatif et symbolique dans le cadre de la protection des données. Il est toutefois essentiel de s'assurer de l'impact que cette règlementation peut avoir sur les activités de Facebook. C'est pourquoi nous commencerons par définir Facebook et son domaine d'activité, pour ensuite analyser l'objet de l'intervention du RGPD. Dans une seconde section nous délimiterons son champ d'application, et nous déterminerons comment le cas de Facebook peut être inclus dans ce champ d'application. Après avoir répondu à ces questions, nous nous interrogerons sur la manière de faire appliquer le RGPD au cas de Facebook.

Section 1 : Considérations préliminaires

§1. Le domaine d'activité de Facebook

Facebook est une plateforme permettant à ses utilisateurs de communiquer « *tous types d'informations, à partir de profils personnalisés* »[25], qui sont mises à disposition des autres utilisateurs « *selon des règles définies en partie par les utilisateurs mais aussi par Facebook* »[26], au moyen de paramètres de confidentialité plus ou moins modulables[27].

Facebook est aussi une entreprise[28]. L'échange d'informations qu'elle provoque via sa plateforme permet insidieusement d'alimenter ses bases de données. Elles font l'objet de traitements automatisés constants, principalement à des fins de ciblage publicitaire[29] comme nous l'aborderons plus en détail dans le second chapitre.

Le siège de Facebook est situé à Menlo Park, en Californie[30]. Cependant ce géant d'Internet dispose d'autres bureaux aux quatre coins des USA, mais aussi aux quatre coins du monde[31]. De

[25] J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, p. 236.
[26] *Ibid*.
[27] *Ibid*., p. 242-243.
[28] *Ibid*.
[29] *Ibid*.
[30] E. PROTALINSKI, *Facebook completes move from Palo Alto to Menlo Park*, ZDNET, le 19 décembre 2011 (article en ligne disponible sur https://www.zdnet.com/article/facebook-completes-move-from-palo-alto-to-menlo-park/, dernière consultation le 06 août 2019).
[31] Facebook Newsroom, *Company Info* (disponible sur https://newsroom.fb.com/company-info/, dernière consultation le 06 août 2019).

nombreuses villes européennes, entre autres, accueillent les bâtiments de Facebook. Facebook quant à lui accueille, au dernier recensement, un milliard et demi d'utilisateurs quotidiens actifs et presque deux milliards et demi d'utilisateurs mensuels actifs à travers le monde[32]. La plateforme est d'ailleurs traduite en plus de cent-dix langues différentes[33]. Autant de preuves tangibles que Facebook n'est pas seulement une entreprise américaine, mais surtout une entreprise internationale.

§2. Le rôle du RGPD dans le paysage législatif

Facebook n'étant pas la seule entreprise suivant ce modèle économique basé sur la monétisation des données personnelles à l'échelle internationale, les normes destinées à protéger ces données se doivent désormais d'avoir une portée tout aussi large[34].

La directive 95/46/CE, abrogée par la mise en application du RGPD[35], tentait déjà de réaliser le même objectif, mais le fait de la remplacer par un règlement a permis d'harmoniser les législations des pays européens[36]. Même si les États se sont vu offrir une certaine marge de manœuvre dans la transposition du RGPD dans leurs législations nationales, celui-ci aspire à une certaine uniformisation[37]. En effet, contrairement à la directive, « *le règlement a vocation à s'appliquer directement sur tout le territoire européen, sans renvoi à une loi nationale* »[38]. Cette ambition permet d'assurer à la fois la libre circulation des données au sein de l'Union Européenne et une protection équivalente des individus, ce qui permet d'éliminer le « *dumping éthique* »[39] – soit la relocalisation d'une activité en fonction du niveau d'éthique d'un pays – qu'occasionnaient les différences de niveau de protection[40].

L'apparition du RGPD a également pour avantage de refléter les évolutions numériques et technologiques ayant eu lieu au cours des vingt dernières années et constitue ainsi une mise à

---

[32] Facebook Newsroom, *Company Info* (en ligne), *op. cit.*
[33] Facebook, *Sélectionner une langue* (disponible sur https://m.facebook.com/language.php, dernière consultation le 06 août 2019).
[34] N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, p. 53.
[35] RGPD, art. 94, §1.
[36] C. PONSART et R. ROBERT, « Le règlement européen de protection des données personnelles », *op. cit.*, p. 422.
[37] *Ibid.*, p. 422.
[38] *Ibid*., p. 423.
[39] N. BINCTIN, « Partie 2 : Créer une patrimonialité des données à droit constant », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles*, (Sous la direction de LÉGER L.), janvier 2018 (disponible sur https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf, dernière consultation le 06 août 2019), p. 77.
[40] *Ibid*.

niveau importante des normes en matière de protection des données[41]. Il permet ainsi d'« *assurer tout leur effet utile aux règles de protection des données dans le contexte d'une industrie numérique mondialisée* »[42].

Cependant, cette industrie-là a majoritairement envahi l'Europe en traversant l'Atlantique, Facebook étant loin d'être le seul géant d'Internet né en Amérique[43]. Et comme nous l'avons démontré dans la section précédente, le marché des GAFA et de leurs semblables s'impose en Europe par la maximisation de leur public cible. C'est pour cette raison que l'Union Européenne s'intéresse de près à ces entreprises, et que Facebook a par exemple été auditionné quelques jours avant la mise en application du RGPD par le Parlement européen[44]. Cela explique également l'étendue du champ d'application du RGPD que nous aurons l'occasion d'analyser en détail dans la section suivante.

Section 2 : L'impact du champ d'application du RGPD sur le cas de Facebook

Le RGPD définit son champ d'application de manière « *unilatérale et explicite* »[45]. Il entend dès lors exclure le règlement bilatéral de conflits de loi au travers de dispositions du droit international privé, même si rien n'empêche de l'envisager dans la pratique[46].

Facebook a par exemple été au cœur d'une telle situation, qui a été tranchée par un récent jugement français du 9 avril 2019 en matière de protection des consommateurs[47]. Les clauses inclues par le réseau social dans sa Déclaration des Droits et Libertés prétendaient affirmer la compétence des juridictions californiennes et l'application du droit californien[48]. Le Tribunal de Grande Instance de Paris a considéré que les clauses de juridiction en question étaient des clauses abusives dans la mesure où le fait d'imposer la compétence des juridictions californiennes aux utilisateurs de Facebook du monde entier était principalement dissuasif et entravait l'accès à une

---

[41] A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op.cit*, p. 20.
[42] C. GAYREL, « Chapitre 12. - L'expansion des standards européens de protection des données dans le monde », *in L'Europe des droits de l'homme à l'heure d'Interne*t, Bruxelles, Bruylant, 2019, p. 476.
[43] J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, pp. 236-237.
[44] N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, p. 53.
[45] *Ibid.*, p. 54.
[46] *Ibid.*
[47] TGI de Paris, 9 avril 2019, (disponible sur https://www.legalis.net/jurisprudences/tgi-de-paris-jugement-du-9-avril-2019/, dernière consultation le 06 août 2019).
[48] *Ibid.*

quelconque justice de par les difficultés pratiques qu'impliquaient ces clauses dans la plupart des cas[49]. En ce qui concerne l'application de la loi californienne, ce tribunal français a estimé que cela allait à l'encontre, entres autres, du Règlement Rome 1, qui prévoit que dans le cadre d'un contrat entre un professionnel et un consommateur, c'est la loi du pays de résidence de ce consommateur qui s'applique au contrat dès lors que le professionnel dirige son activité vers ce pays[50]. Ce même règlement n'empêche pas les contrats de consommation de prévoir une clause de choix de loi mais ne permet pas de priver les consommateurs de la protection qui leur est octroyée par la loi de leur pays de résidence[51]. Il est en effet indéniable que Facebook oriente son activité vers la France et vers l'Europe dans son ensemble, comme nous l'avons prouvé précédemment. En guise de défense, Facebook a prétendu que ses services étant dispensés gratuitement, on ne pouvait parler d'un contrat de consommation et que les arguments de l'association de défense de consommateurs qui l'attaquait en l'occurrence[52] n'étaient donc pas valables. Le Tribunal a considéré que la monétisation des données personnelles opérée par Facebook, que nous avons évoquée précédemment, était suffisante pour qualifier la relation entre Facebook et ses utilisateurs de contrat de consommation et que l'application des normes destinées à protéger les consommateurs étaient applicable au cas d'espèce[53].

Le jugement en question a réglé de nombreuses questions relatives à la validité des conditions générales d'utilisation de Facebook, la protection des données constituant l'un des enjeux principaux de ce procès ayant commencé en 2014[54].

Le règlement, tout comme la directive avant lui, tient à éviter de tels débats. C'est pourquoi l'exploiter comme fondement juridique peut s'avérer être stratégiquement intéressant, pour les individus comme pour les associations. Pourtant, malgré la volonté du Parlement et de la Commission de couvrir un panel de situations relativement large, certaines difficultés subsistent quant à la détermination du champ d'application du règlement qu'ils ont produit[55]. Il semble donc

---

[49] TGI de Paris, 9 avril 2019, (disponible sur https://www.legalis.net/jurisprudences/tgi-de-paris-jugement-du-9-avril-2019/, dernière consultation le 06 août 2019).
[50] Règlement (CE) n° 593/2008 du Parlement européen et du Conseil du 17 juin 2008, sur la loi applicable aux obligations contractuelles (Règlement Rome I), *J.O.U.E.*, L 177, du 4 juillet 2008, p. 006, art 6.1.
[51] *Ibid.*, art 6.2.
[52] G. RUE, « Facebook doit changer ses conditions d'utilisation », *B.S.J.*, 2019/629, p. 11.
[53] TGI de Paris, 9 avril 2019, (disponible sur https://www.legalis.net/jurisprudences/tgi-de-paris-jugement-du-9-avril-2019/, dernière consultation le 06 août 2019).
[54] G. RUE, « Facebook doit changer ses conditions d'utilisation », *op. cit.*, p. 11.
[55] N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, p. 52.

nécessaire de s'assurer qu'il s'applique au cas qui nous intéresse, à savoir les activités de Facebook. Nous répondrons à cette question en trois temps, en analysant successivement le champ d'application matériel, le champ d'application personnel et le champ d'application territorial de ce texte.

§1. Le champ d'application matériel

La question est ici de déterminer les activités qui rentrent dans le cadre de la réglementation. L'article 2 du RGPD entend élargir le champ d'application matériel « *au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier* »[56].

Le traitement est défini comme « *toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel* »[57]. Les procédés automatisés regroupent toutes les « *technologies informatiques permettant de traiter des données* »[58], actuelles et à venir[59]. À l'exception – somme toute minime – du « *traitement manuel non structuré* »[60], toutes les opérations impliquant des données personnelles relèvent du RGPD[61].

Le concept de "donnée à caractère personnel" est également de nature à élargir l'ensemble des hypothèses couvertes par le RGPD, puisqu'il inclut « *toute information se rapportant à une personne physique identifiée ou identifiable* »[62]. Le Groupe de Travail de l'Article 29, aujourd'hui appelé « *Comité Européen de la Protection des Données* »[63], avait décortiqué en 2007 cette définition qui existait déjà dans le texte de la directive 95/46/CE[64]. Cette analyse est donc toujours d'actualité[65]. Dans l'expression "toute information", le Groupe de Travail de l'Article 29 inclut toute information de nature objective ou subjective, correcte ou incorrecte, quel que soit son contenu et

---

[56] RGPD, art. 2, §1.
[57] *Ibid.*, art. 4, §2.
[58] A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, p. 16.
[59] *Ibid.*
[60] N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, p. 55.
[61] *Ibid.*
[62] RGPD, art. 4, §1.
[63] *Ibid.*, art. 94, §2 et art. 68 et s.
[64] N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, p. 55.
[65] RGPD, art. 94, §2

sous n'importe quel format[66]. Le Groupe de Travail de l'Article 29 a également établi les critères alternatifs permettant d'identifier ce qui "se rapporte" à un individu sur base de la formulation d'un de leurs écrits antérieurs : « *les données concernent une personne si elles ont trait à l'identité, aux caractéristiques ou au comportement d'une personne ou si cette information est utilisée pour déterminer ou influencer la façon dont cette personne est traitée ou évaluée* »[67]. L'information doit donc présenter un critère de contenu, un critère de finalité ou un critère d'effet pour que la donnée se rapporte à un individu[68]. La Cour de Justice de l'Union Européenne (ci-après appelée C.J.U.E.) a confirmé l'application de ces critères[69]. Quant au rapport à une "personne physique identifiée ou identifiable", il implique que l'information ait la capacité, seule ou combinée à d'autres informations[70], d'identifier un individu[71]. L'information doit donc avoir « *une relation particulièrement privilégiée et étroite avec la personne physique concernée* »[72]. La C.J.U.E. a précisé la nécessité de « *moyens susceptibles d'être raisonnablement mis en œuvre soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne* »[73] pour que l'information puisse être qualifiée d'identifiable. Dans l'hypothèse où il serait « *matériellement impossible – ou au prix d'efforts disproportionnés compte tenu de la nature des données –* »[74] d'individualiser une personne au moyen de celles-ci, le RGPD n'a pas à s'appliquer puisqu'elles sont dite anonymisées[75]. Ce concept est à utiliser avec précaution puisque le développement constant des technologies et des bases de données implique la possibilité qu'une donnée considérée comme anonymisée devienne une donnée à caractère personnel par réidentification[76]. Il ne faut donc pas automatiquement déduire de l'anonymisation d'une donnée l'inapplicabilité du RGPD[77].

Le RGPD liste les données susceptibles d'identifier une personne physique : « *un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs*

---

[66] Avis n° 4/2007 du Groupe de Travail de l'Article 29 sur le concept de données à caractère personnel, WP 136, 20 juin 2007 (10107/05/FR) pp. 6-10.
[67] Document de travail du Groupe de Travail de l'Article 29 sur les questions de protection des données liées à la technologie RFID (radio-identification), WP 105, 19 janvier 2005 (01248/07/FR), p. 9.
[68] Avis n° 4/2007 du Groupe de Travail de l'Article 29 sur le concept de données à caractère personnel, WP 136, 20 juin 2007 (10107/05/FR) p. 11.
[69] Arrêt Peter Nowak/Data Protection Commissioner, C-434/16, EU:C:2017:994, pt.35.
[70] Arrêt Patrick Breyer/Bundesrepublik Deutschland, C−582/14, EU:C:2016:779, pt.32
[71] N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, pp. 56-57.
[72] Avis n° 4/2007 du Groupe de Travail de l'Article 29 sur le concept de données à caractère personnel, WP 136, 20 juin 2007 (10107/05/FR) p. 13.
[73] Arrêt Patrick Breyer/Bundesrepublik Deutschland, C−582/14, EU:C:2016:779, pt.41
[74] A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, pp. 17-18
[75] RGPD, cons. 26.
[76] A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, p. 19.
[77] *Ibid.*

éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »[78]. Toutefois, il est essentiel de préciser qu'il ne faut pas nécessairement qu'une donnée soit relative à la vie privée de quelqu'un, ou confidentielle pour être considéré comme "donnée à caractère personnel" au regard du règlement[79]. Il peut s'agir d'informations déjà rendues publiques, ou bien de données concernant la vie professionnelle de la personne[80]. L'information peut également être « *indirectement relative à une personne* »[81], c'est-à-dire concerner un élément de son entourage proche.

Le domaine d'activité de Facebook semble correspondre trait pour trait à ce premier canevas. Les traitements effectués par Facebook étant réalisés au travers de son site Internet, et en aucun cas de manière manuelle non-structurée, ils sont toujours considérés comme automatisés[82]. Quant aux données qu'il rassemble et utilise, ce sont entre autres celles que les individus fournissent eux-mêmes, à leur propos, au travers de leur profil personnalisé. Ils sont donc facilement identifiables par la plateforme. Nous pouvons donc aisément nous rassurer sur l'inclusion de Facebook dans le champ d'application matériel du RGPD. De plus, Facebook ne rentre dans aucune des exceptions particulières prévues par l'article 2 du règlement, hormis peut-être celle qui exclut les activités n'étant pas soumise au droit de l'Union Européenne[83]. Nous répondrons à cette question dans le troisième paragraphe de cette section.

§2. Le champs d'application personnel

Le RGPD s'applique aux responsables du traitement et à leurs sous-traitants[84].

Le responsable du traitement est défini comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* »[85]. Le Groupe de Travail de l'Article 29 utilise l'expression de

---

[78] RGPD, art. 4, §1
[79] A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, p. 17.
[80] *Ibid.*
[81] *Ibid.*
[82] J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, pp. 242-243.
[83] RGPD, art. 2, §2, a).
[84] *Ibid.*, art. 3.
[85] *Ibid.*, art. 4, §7

« *maître du fichier* »[86]. Le fait de "déterminer les finalités et les moyens" est une « *question d'influence* »[87]. C'est effectivement l'influence sur ce qui essentiel à la détermination du "pourquoi" et du "comment"[88] du traitement qui compte en l'espèce[89], et la C.J.U.E. prétend entendre largement l'interprétation de ce concept d'influence[90]. Le seuil en-dessous duquel elle ne serait pas suffisante que pour qualifier celui qui l'exerce de responsable du traitement semble être fixé par « *un pouvoir de décision s'étendant au-delà des seules questions techniques et d'organisation que sont, par exemple, le choix du matériel informatique ou celui du logiciel à utiliser pour collecter, stocker ou transférer les données* »[91].

On peut considérer que Facebook représente en tant que personne morale le responsable du traitement des données qu'elle collecte puisqu'elle décide à la fois de la manière dont sont traitées les données et de l'objectif final de ce traitement[92], à savoir en tirer un avantage économique. C'est la société en elle-même qui « *définit techniquement et contractuellement les gammes de finalités et les outils informatiques de traitement de données qu'elle met en place via son service* »[93]. C'est également elle qui « *fixe et modifie les conditions d'utilisation* »[94]. Le Groupe de Travail de l'Article 29 considère d'ailleurs généralement les fournisseurs de réseaux sociaux comme étant responsables du traitement[95]. Le titre de responsable du traitement implique un rôle particulier, à savoir celui de « *faire respecter les règles de protection des données, et comment les personnes concernées peuvent exercer leurs droits dans la pratique* »[96].

L'existence de responsables conjoints est délicate à fixer dans le cas de Facebook. Le responsable conjoint serait une personne physique ou morale en mesure et en position d'avoir une

---

86 Avis n° 1/2010 du Groupe de Travail de l'Article 29 sur les notions de responsable du traitement et de sous-traitant, WP 169, 16 février 2010 (00264/10/FR), p. 4.
87 N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, p. 59.
88 A. DELFORGE, « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *in Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Larcier, 2018, p. 376.
89 Avis n° 1/2010 du Groupe de Travail de l'Article 29 sur les notions de responsable du traitement et de sous-traitant, WP 169, 16 février 2010 (00264/10/FR), p. 14.
90 Arrêt Tietosuojavaltuutettu, C-25/17, EU:C:2018:551, pt.68.
91 N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, p. 59.
92 J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, pp. 254-255.
93 *Ibid.*, p. 249.
94 *Ibid.*
95 Avis n° 5/2009 du Groupe de Travail de l'Article 29 sur les réseaux sociaux en ligne, WP 163, 12 juin 2009 (01189/09/FR), p. 5.
96 Avis n° 1/2010 du Groupe de Travail de l'Article 29 sur les notions de responsable du traitement et de sous-traitant, WP 169, 16 février 2010 (00264/10/FR), p. 4.

influence sur la manière et les raisons de Facebook de traiter les données collectées sur sa plateforme[97]. Pour de simples administrateurs de pages qui paramètreraient des publicités ciblées, Facebook Ireland a récemment décidé dans un « *Addenda concernant le responsable de traitement des données Statistiques* »[98] des pages Facebook, de « *prendre la responsabilité principale en vertu du RGPD pour le traitement des données statistiques* »[99], et précise que seul lui peut « *prendre et mettre en œuvre des décisions concernant le traitement des données statistiques* »[100]. Cependant, cet accord ne vaut que s'il correspond à la réalité[101] : « *la désignation dans un contrat d'une partie comme responsable du traitement ne suffit donc pas pour qualifier celle-ci de responsable du traitement au sens du droit relatif à la protection des données* » [102]. De plus, la C.J.U.E. a décidé que le rôle de responsable du traitement inclut également l'administrateur de page fan[103], dès lors qu'il a la possibilité de « *définir les critères à partir desquels ces statistiques doivent être établies et même désigner les catégories de personnes qui vont faire l'objet de l'exploitation de leurs données à caractère personnel par Facebook* »[104], sans qu'il soit nécessaire que cette possibilité ait été mise à profit[105]. On pourrait envisager que les annonceurs publicitaires de Facebook remplissent aussi les critères nécessaires pour avoir une responsabilité équivalente à celle de Facebook quant à l'utilisation des données personnelles en jeu en matière de ciblage publicitaire[106].

Quant au sous traitant il est défini comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement* »[107]. Si Facebook fait appel à des sous-traitants en traitement de données, notamment afin d'entraîner les algorithmes et l'intelligence artificielle du réseau social[108], le réseau social agit également parfois en qualité que sous-traitant. C'est du moins ce qu'il

---

97 RGPD, art. 26, §1.
98 Facebook, *Addenda concernant le responsable de traitement des données Statistiques* (disponible sur https://www.facebook.com/legal/terms/page_controller_addendum, dernière consultation le 06 août 2019).
99 *Ibid.*
100 *Ibid.*
101 RGPD, art. 26, §2.
102 A. DELFORGE, « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.*, 2018, p. 375.
103 Arrêt Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein GmbH (arrêt Fanpage), C-210/16, EU:C:2018:388., pt 44.
104 *Ibid.*, pt.36.
105 N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, p. 60.
106 J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, pp. 254-255.
107 RGPD, art. 4, §8.
108 L. B., *Les sous-traitants de Facebook lisent vos posts privés pour entraîner l'IA*, Le Big Data, le 6 mai 2019 (article en ligne disponible sur https://www.lebigdata.fr/sous-traitants-facebook-posts-prives, dernière consultation le 06 août 2019).

prétend dans une de ses déclarations concernant sa fonctionnalité Facebook Business[109]. Il est par exemple établi dans cette publication que Facebook agit en qualité de sous-traitant lorsqu'il crée une audience personnalisée pour une firme en comparant les informations de sa propre base de données à celles fournies par la firme en question[110]. C'est également ce qui est fixé lorsque Facebook analyse les données des informations de sa propre base de données à des fins statistiques, dans le but d'informer un annonceur sur l'efficacité de ses publicités ciblées[111]. Ces déclarations mériteraient probablement une analyse plus approfondie par une autorité ou une cour compétente. Il est indéniable que dans les hypothèses présentées, Facebook agit pour le compte d'autres entreprises. Néanmoins, il y a lieu de se demander s'il n'agit pas également à son propre avantage en traitant ces données, notamment afin d'améliorer son interface et d'augmenter le rendement des bannières publicitaires qu'il propose dans leur ensemble. Tout comme pour le rôle de responsabilité conjointe, celui de sous-traitance se définit par rapport à la réalité des faits et pas uniquement par ce qui est prévu par accord[112]. Quoi qu'il en soit, le texte du RGPD assure « *un resserrement des obligations entre "responsable de traitement" (...) et "sous-traitants" (...)* »[113] en obligeant chacun de ces acteurs à œuvrer pour le respect des exigences du règlement[114]. Pour les besoins de cette étude, nous nous en tiendrons au fait que Facebook, comme il le reconnaît lui-même, agit la plupart du temps comme responsable du traitement[115].

§3. Le champ d'application territorial

L'article 3 du RGPD distingue deux hypothèses distinctes. L'une où le responsable de traitement est établi sur le territoire de l'union et l'autre où ce n'est pas le cas. En ce qui concerne Facebook, nous savons déjà que l'entreprise dispose de bureaux dans plusieurs pays d'Europe, celui de Dublin semblant être central[116] : Facebook l'a effectivement élevé au rang d'« *International*

---

[109] Facebook Business, *Qu'est-ce que le Règlement général sur la protection des données (RGPD)* ? (disponible sur https://www.facebook.com/business/gdpr, dernière consultation le 06 août 2019).
[110] *Ibid.*
[111] *Ibid.*
[112] A. DELFORGE, « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.*, p. 375.
[113] N. BINCTIN, « Partie 2 : Créer une patrimonialité des données à droit constant », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles* (en ligne)*, op. cit.*, p. 82.
[114] *Ibid.*
[115] Facebook Business, *Qu'est-ce que le Règlement général sur la protection des données (RGPD)* ? (en ligne), *op. cit.*
[116] J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, p. 238.

Headquarters »[117]. C'est pour cette raison que c'est la première hypothèse de l'article 3 qui nous intéresse particulièrement ici.

Celle-ci étend la portée du RGPD « *au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union* »[118]. Si le règlement définit ce qu'elle considère être un « *établissement principal* »[119] lorsqu'une entreprise dispose de plusieurs établissements en Europe, aucun article ne précise ce qui correspond à un simple établissement[120]. Comme souvent, c'est dans les considérants qu'il faut chercher les précisions nécessaires à la compréhension des subtilités du RGPD. L'un de ceux-ci énonce que cela « *suppose l'exercice effectif et réel d'une activité au moyen d'un dispositif stable* »[121], sans égard pour la forme juridique de ce dispositif[122]. La directive 95/46/CE utilisait déjà les mêmes critères, et dans le cadre d'une affaire antérieure à la mise en application du RGPD, la C.J.U.E. a retenu une « *conception souple de la notion d'établissement, qui écarte toute approche formaliste selon laquelle une entreprise ne serait établie que dans le lieu où elle est enregistrée* »[123] et précise que « *cela vaut tout particulièrement pour des entreprises qui s'emploient à offrir des services exclusivement sur Internet* »[124]. Les bureaux de Facebook à Dublin semblent remplir largement ces exigences fixées par la législation et la jurisprudence.

La manière dont la rédaction de cette disposition est centrée sur l'établissement du responsable de traitement, est pour le moins étonnante car elle n'évoque nullement les personnes auxquelles se rapportent les données traitées[125]. Cela signifie « *qu'aucun lien de connexion entre la personne concernée et l'Union n'est requis pour l'application de ce point* »[126]. « *Toute personne* »[127] compte,

---

[117] Facebook Newsroom, *Facebook to Establish International Headquarters in Dublin, Ireland*, le 2 octobre 2008 (article disponible sur https://newsroom.fb.com/news/2008/10/facebook-to-establish-international-headquarters-in-dublin-ireland/, dernière consultation le 06 août 2019).
[118] RGPD, art. 3, §1.
[119] *Ibid.*, art. 4, §16.
[120] N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, p. 65.
[121] RGPD, cons. 22.
[122] *Ibid.*
[123] Arrêt Weltimmo s. r. o./Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, EU:C:2015:639, pt.29.
[124] *Ibid.*
[125] N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, p. 66.
[126] *Ibid.*
[127] Traité sur le Fonctionnement de l'Union européenne (version consolidée), J.O.U.E., C 326, du 26 octobre 2012, p. 001, art. 16 ; Charte des Droits Fondamentaux de l'Union Européenne, J.O.U.E., C 326, du 26 octobre 2012, p. 391, art. 8.

sans distinction à l'égard de sa nationalité ou de son lieu de résidence[128], tant qu'elle est en mesure de démontrer que « *le traitement a lieu dans le cadre des activités d'un établissement sur le territoire de l'Union* » [129]. Si cette condition est remplie, le RGPD sera d'application, peu importe le lieu où les données sont réellement traitées[130]. C'est une précision apportée par le règlement par rapport à ce qui était prévu dans la directive[131].

Le problème que nous pose la première hypothèse de l'article 3, consiste à savoir quels traitements sont effectués "dans le cadre des activités" des quartiers de Dublin, et sont donc soumis aux exigences du règlement. Comme nous venons de le préciser, l'hypothèse selon laquelle le traitement n'aurait pas lieu au sein de cet établissement en Europe, ou même que les données n'y seraient pas directement accessibles n'est en aucun cas déterminant[132]. Le RGPD confirme l'avis de la C.J.U.E.[133], qui a estimé, dans le cadre d'un procès impliquant Google et l'une de ses filiales[134], que le texte de la directive 95/46/CE allait dans ce sens.

Les critères permettant de déterminer si un traitement entre dans "le cadre des activités" d'un établissement secondaire sont les suivants[135] : il faut tout d'abord évaluer « *le degré de participation de l'établissement aux activités de traitement, la nature des activités, ainsi que la nécessité d'assurer la protection effective des données* »[136], puis vérifier s'il existe un « *lien indissociable* »[137] entre ces activités et le traitement. Dans le cadre de l'affaire évoquée ci-dessus, la C.J.U.E. a estimé qu'en ce qui concerne la filiale de Google établie en Espagne, ce lien entre le traitement de données de Google et « *la promotion et la vente des espaces publicitaires proposés par ce moteur* »[138] par Google Spain était bien présent, étant donné que ces activités « *constituent le*

---

[128] N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, p. 66.
[129] *Ibid.*
[130] A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, pp. 19-20.
[131] T. VAN CANNEYT, « The general data protection regulation : 10 things company lawyers should know », *op. cit.*, p. 1.
[132] N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, p. 67.
[133] *Ibid.*
[134] Arrêt Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12, EU:C:2014:317, pt.60.
[135] N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, p. 68.
[136] Avis n° 8/2010 du Groupe de Travail de l'Article 29 sur le droit applicable, WP 179, 16 décembre 2010, (0836-02/10/FR), p. 2.
[137] Update of Opinion 8/2010 of the Working Party 29 on applicable law in light of the CJEU judgment in Google Spain, WP 179 update, 16 décembre 2015 (176/16/EN), p. 8.
[138] Arrêt Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12, EU:C:2014:317, pt.60.

*moyen pour rendre le moteur de recherche en cause économiquement rentable et que ce moteur est, en même temps, le moyen permettant l'accomplissement de ces activité*s »[139]. Il est également intéressant de constater que la C.J.U.E. ajoute qu'il faut qu'une activité *« vise les habitants de cet État membre* »[140] et donc que « *la direction des activités de l'établissement joue un rôle pour déterminer si le traitement en cause a bel et bien été effectué dans le cadre de son activité* »[141].

Nous pouvons donc considérer que Facebook Ireland, société « *spécialisée dans le secteur d'activité du traitement de données, hébergement et activités connexes* »[142] est soumise à cette première hypothèse. D'autant plus que l'objectif de ces "bureaux internationaux" est de viser les utilisateurs d'Europe (mais aussi d'Afrique et du Moyen Orient)[143]. Mais il est compliqué de déterminer avec exactitude quels traitements de données sont réalisés « *dans le cadre du fonctionnement de la "branche communautaire" du réseau social* »[144].

Toutefois, même dans le cas où les bureaux européens de Facebook n'existeraient pas, le traitement de données opérée par l'entreprise rentrerait dans le champ d'application territorial de la directive 95/46/CE. Effectivement la seconde hypothèse couvre les cas où il n'y a pas d'établissement en Europe, mais dans ce cas l'utilisateur concerné par le traitement de données doit nécessairement se trouver sur le territoire de l'Union. Elle a été envisagée afin « *d'éviter que le responsable du traitement puisse échapper à l'application du GDPR en contournant le point 1* »[145]. Elle prévoit donc deux possibilités pour que le RGPD trouve à s'appliquer à une entreprise qui n'a aucun "dispositif stable" en Europe : « *l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes »*[146] *et le « suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union* »[147]. Il est indéniable que Facebook rencontre ces deux cas de figure. Le premier bien évidemment, dans la mesure où le réseau social offre une plateforme gratuite aux utilisateurs

---

[139] Arrêt Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12, EU:C:2014:317, pt.56.
[140] *Ibid.*, pt.60.
[141] N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, p. 68.
[142] Fiche d'entreprise de Facebook Ireland (disponible sur https://www.societe.com/societe/facebook-ireland-limited-814665519.html dernière consultation le 06 août 2019).
[143] Facebook Newsroom, *Facebook to Establish International Headquarters in Dublin, Ireland*, (en ligne), *op. cit*.
[144] J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, p. 261.
[145] N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, p. 66.
[146] RGPD, art. 3, §2, a).
[147] *Ibid.*, art. 3, §2, b).

Européens, qui comme nous l'avons vu est disponible en de nombreuses langues, dont plusieurs pratiquées en Europe[148]. Le second également puisque, comme nous le verrons de manière détaillée dans le deuxième chapitre, Facebook effectue un traçage des internautes afin d'améliorer son profilage publicitaire.

La troisième et dernière hypothèse envisagée par le règlement est celle du « *traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public* »[149]. Elle n'a aucun impact sur les activités de Facebook et n'est donc pas nécessaire à notre analyse.

L'étendue du champ d'application territorial du RGPD est pour le moins surprenant et peut fortement contrarier les entreprises étrangères visant le marché Européen, ainsi que les pays les hébergeant, qui se sentent quelque peu envahis par cette législation Européenne (ce qui était déjà le cas sous le régime de la directive 95/46/CE, mais avec des sanctions beaucoup moins importantes)[150]. Néanmoins, au vu de la globalisation à laquelle nous assistons aujourd'hui, une telle extraterritorialité du RGPD était essentielle pour que les normes en matière de protection des données personnelles aient l'effet escompté en Europe, même si elle se doit de s'appliquer de manière proportionnelle[151].

Un problème subsiste tout de même dans la détermination des dispositions applicables[152]. Une entreprise comme Facebook peut très bien rentrer dans les conditions de l'article 3, mais dépendre également des dispositions réglant les transferts internationaux de données[153] dans la mesure ou l'article 3 n'a pas égard au lieu où les données sont traitées[154]. Le transfert de données entre Facebook Ireland et Facebook Inc. aux États-Unis pourrait donc dépendre de ces deux régimes[155]. À cet égard, le RGPD prévoit qu'un transfert peut avoir lieu vers un pays tiers sans autorisation

---

148 Facebook, *Sélectionner une langue* (en ligne), *op. cit.*
149 RGPD, art. 3, §3.
150 N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, p. 71.
151 *Ibid.*, p. 71-72.
152 *Ibid.*, p. 73-74.
153 RGPD, art. 44-50.
154 N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, pp. 73-74.
155 *Ibid.*

spécifique[156] lorsqu'il est établi que ce pays « *assure un niveau de protection adéquat* »[157]. Le "Bouclier de Protection", décision de la commission autorisant le transfert de données personnelles de l'Europe aux État-Unis[158], a été mis en place sous le régime de la directive[159] et reste en vigueur sous celui du règlement[160]. Facebook est une des nombreuses entreprises comprises dans cet accord[161]. Toutefois le scandale de l'affaire Cambridge Analytica, que nous développerons dans le chapitre suivant, est de nature à remettre cette décision en question. La C.J.U.E devra se prononcer sur cette question dans les mois à venir[162].

§4. L'application du RGPD dans la pratique

Des recours juridictionnels à l'encontre d'un responsable de traitement sont toujours envisageables, mais les difficultés qu'impliquent une procédure judiciaire ont généralement tendance à être dissuasives : les coûts engendrés, la durée souvent excessive du processus et les problèmes de procédure sont autant de freins pour les individus. Dans une affaire ayant eu lieu en Belgique entre 2015 et 2016[163], le juge des référés du Tribunal de Première Instance de Bruxelles a condamné Facebook à cesser de tracer les internautes à leur insu, et ce sous astreinte, sur base d'une demande introduite par La Commission de Protection de la Vie Privée (CPVP)[164]. Mais Facebook a bien évidemment introduit un recours en Cour d'Appel. Celle-ci a décidé de ne pas se reconnaître de compétence internationale pour traiter d'une affaire concernant Facebook Inc et Facebook Ireland et a considéré qu'une procédure en référé n'était pas justifiée à l'encontre de Facebook Belgium en l'occurrence puisque la condition d'urgence n'était pas rencontrée[165], la pratique reprochée à Facebook par la CPVP ayant cours depuis 2012[166]. Le jugement du Tribunal de Première Instance a donc été réformé, et pour des questions de procédure, c'est la protection des

---

156 RGPD, art. 45, §1.
157 *Ibid.*
158 Décision d'exécution (UE) 1250/2016 de la Commission du 12 juillet 2016, conformément à la directive 95/46/CE du Parlement européen et du Conseil, relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, notifiée sous le numéro C/2016/4176, *J.O.U.E.*, L 207, du 1er août 2016, p. 001.
159 Directive (CE) n° 46/1995, art. 25, §6.
160 RGPD, art. 96.
161 Privacy Shield Framework, Facebook Inc. Participation (disponible sur https://www.privacyshield.gov/participant?id=a2zt0000000GnywAAC, dernière consultation le 06 août 2019).
162 Demande de décision préjudicielle à la C.J.U.E présentée par la High Court (Irlande), Data Protection Commissioner / Facebook Ireland Limited, Maximilian Schrems, C-311/18, *J.O.U.E.*, C 249, du 16 juillet 2018, p. 15.
163 G. DEJEMEPPE, « L'affaire Facebook : questions de procédure », *R.D.T.I.*, 2016/1, n° 62, p. 113.
164 Civ. Bruxelles nl. (réf.), 9 novembre 2015, *J.L.M.B*., 2017, liv. 26, p. 1240.
165 Bruxelles nl. (18e ch.), 29 juin 2016, *J.L.M.B.*, 2017 (sommaire), liv. 26, p.1249.
166 E. DEGRAVE, *Facebook, les cookies et la justice belge : le retour,* le 22 mars 2018 (article en ligne disponible sur http://www.justice-en-ligne.be/article1044.html?utm_source=moteur_jel&utm_medium=thematique&utm_campaign=recherche, dernière consultation le 06 août 2019).

données personnelles et des individus qui a été négligée. Néanmoins, comme nous le verrons, la CVP ne s'est pas arrêtée là pour autant.

L'existence d'autorités publiques indépendantes[167], appelées Autorités de Protection des Données (APD), dans chaque pays de l'Union[168] est de nature à simplifier et à accélérer le processus et à encourager les individus à faire valoir leurs droits[169]. Les individus peuvent s'en remettre à une APD dans le cas où ils estiment qu'une violation du RGPD a lieu et qu'elle est de nature à leur porter préjudice[170]. Ces autorités de contrôle, qui existaient déjà sous le régime de la directive 95/46/CE, sont considérées comme un « *élément essentiel de la protection des personnes physiques à l'égard du traitement des données à caractère personnel* »[171]. Elles se sont récemment vu octroyer des pouvoirs supplémentaires afin de pouvoir faire appliquer les nouveautés introduites par le RGPD[172].

Les APD ont pour rôle de « *surveiller l'application du présent règlement, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union* »[173]. Leur mission est donc d'assurer l'équilibre entre les deux objectifs clé du règlement, soit la libre circulation des données et leur protection, qui peuvent pourtant sembler antagonistes[174]. Pour ce faire, chacune d'entre elles est compétente « *pour exercer les missions et les pouvoirs dont elle est investie conformément au présent règlement sur le territoire de l'État membre dont elle relève* »[175]. Les missions en question sont nombreuses et variées et vont du contrôle de l'application du règlement au soutien et à l'information des individus[176]. Leur accomplissement est gratuit[177], hormis dans le cas de demandes « *manifestement infondées ou excessives* »[178]. Les APD disposent de multiples pouvoirs[179] pour mettre ces missions à exécution, mais le plus impressionnant d'entre eux est celui d'imposer des

---

167 RGPD, art. 4, §21.
168 *Ibid.*, art. 51, §1.
169 E. DEGRAVE, *Facebook, les cookies et la justice belge : le retour* (en ligne)*, op. cit.,*
170 RGPD, art. 77, §1.
171 *Ibid.,* cons. 117.
172 D. VAN BRIEL et A. VAN DE MEULEBROUCKE, *Commission vie privée devient Autorité de Protection des Données* (en ligne), *op. cit.*
173 RGPD, art. 51, §1.
174 J.-F. PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *op. cit.*, pp. 41-42.
175 RGPD, art. 55, §1.
176 *Ibid.*, art. 57, §1, a)-v).
177 *Ibid.*, art. 57, §3.
178 *Ibid.*, art. 57, §4.
179 *Ibid.*, art. 58.

sanctions lourdes sous forme d'amendes administratives[180]. Le montant de celles-ci peut désormais « *s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu* »[181]. Pourtant le montant de ces sanctions n'a pas pour objectif « *de faire des autorités de régulation des organes répressifs* »[182], mais bien d'assurer la coopération entre les entreprises et les APD dans le processus de mise en conformité[183].

La Commission Nationale de l'Informatique et des Libertés (CNIL), APD française a récemment inauguré ces nouveaux plafonds en infligeant une amende d'un montant de 50 000 000 d'euros[184] à l'entreprise Google sur base d'une réclamation de deux associations de protection des droits des individus sur Internet[185]. Les plaintes avaient plusieurs fondements : « *manque de transparence, information insatisfaisante et absence de consentement valable pour la personnalisation de la publicité* »[186]. Nous analyserons ces exigences plus en détail dans le cadre du troisième chapitre.

Néanmoins la question de compétence se pose toujours. Celle des APD est réglée par le RGPD. L'introduction du « *mécanisme de guichet unique* »[187] a pour intérêt de permettre aux responsables de traitement de n'avoir affaire qu'à une seule autorité nationale à la fois. Il s'agira normalement de celle de son établissement principal en Europe, appelée autorité chef de file[188]. Cependant chaque APD est compétente pour les affaires relevant de son État membre[189]. En cas de transfert transfrontalier de données personnelles, c'est l'autorité chef de file qui est compétente[190]. Une coopération et une communication efficace entre les autorités des différents pays d'Europe est requise[191].

---

[180] RGPD, cons. 150.
[181] *Ibid.*, art. 83.
[182] A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, pp. 309.
[183] *Ibid.*
[184] GDPR Enforcement Tracker de la CMS (disponible sur http://www.enforcementtracker.com, dernière consultation le 06 août 2019).
[185] Site officiel de la CNIL, *La formation restreinte de la CNIL prononce une sanction de 50 millions d'euros à l'encontre de la société Google LLC*, le 21 janvier 2019 (article en ligne disponible sur https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la, dernière consultation le 06 août 2019).
[186] *Ibid.*
[187] RGPD, cons. 127.
[188] *Ibid.*, cons. 124.
[189] *Ibid.*, art. 55, §1.
[190] *Ibid.*, art. 56.
[191] *Ibid.*, art. 60-62 et cons 127.

En ce qui concerne la compétence des juridictions, la directive 95/46/CE ne réglait pas la question et le RGPD ne comble pas cette lacune[192]. Dans l'affaire évoquée ci-dessus, la CPVP a été déboutée de sa demande en référé pour défaut d'urgence et la question de la compétence des juridictions belges posait clairement problème[193]. En février 2018, le Tribunal de Première Instance de Bruxelles a considéré, au cours d'une procédure au fond cette fois[194], qu'il y avait un lieu de se baser sur la jurisprudence de l'arrêt de la C.J.U.E. concernant Google et sa filiale espagnole[195] et que le fait que Facebook suivait le comportement de ses utilisateurs sur le territoire Belge fondait sa compétence[196]. En degré d'appel, la Cour de Bruxelles a décidé en mai 2019 de s'en remettre à l'avis de la C.J.U.E. en lui posant une question préjudicielle[197] afin de « *savoir si la procédure introduite devant les juridictions civiles par l'APD pouvait se poursuivre compte tenu des règles européennes en vigueur* »[198] et de la création du concept de guichet unique. Il est envisageable que ce mécanisme ait un « *un impact sur la possibilité d'entamer des procédures devant un tribunal* »[199]. Il est donc possible que cette affaire soit finalement prise en charge par l'APD Irlandaise, la *Data Protection Commission of Ireland*[200].

---

192 G. DEJEMEPPE, « L'affaire Facebook : questions de procédure », *R.D.T.I.*, 2016/1, n° 62, pp.116-117.
193 *Ibid.*, p. 113.
194 Civ. Bruxelles nl. (24e ch.), 16 février 2018, *R.A.B.G.*, 2019, liv. 9, p. 695.
195 Arrêt Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12, EU:C:2014:317.
196 Civ. Bruxelles nl. (24e ch.), 16 février 2018, *R.A.B.G.*, 2019, liv. 9, p. 695.
197 Site officiel de l'APD Belge, *La Cour d'appel de Bruxelles réfère l'affaire Facebook à la Cour de justice de l'Union européenne*, le 8 mai 2019 (article en ligne disponible sur https://www.autoriteprotectiondonnees.be/news/la-cour-dappel-de-bruxelles-refere-laffaire-facebook-a-la-cour-de-justice-de-lunion, dernière consultation le 06 août 2019).
198 T. DERIDDER, *Affaire APD contre Facebook – la CJUE saisie !*, le 13 mai 2019 (article en ligne disponible sur https://equal-partners.eu/actualites/affaire-apd-contre-facebook-la-CJUE-saisie, dernière consultation le 06 août 2019).
199 https://www.autoriteprotectiondonnees.be/news/la-cour-dappel-de-bruxelles-refere-laffaire-facebook-a-la-cour-de-justice-de-lunion
200 Site officiel de l'APD Belge, *La Cour d'appel de Bruxelles réfère l'affaire Facebook à la Cour de justice de l'Union européenne* (en ligne), *op. cit.*

Chapitre 2 : Le profilage publicitaire et l'utilisation qu'en fait Facebook

Le profilage relève du « *monde de l'invisible et de l'immatériel* »[201]. Cette pratique ainsi que les nombreux concepts y afférents semblent donc particulièrement abstraits. C'est pour cette raison qu'avant d'aborder les règles spécifiques applicables à l'ensemble des procédés que regroupe le profilage publicitaire, il est essentiel de se faire une idée plus précise de ce qu'il implique et de la manière dont il est réalisé. C'est ce que nous tenterons de faire tout au long de ce chapitre, en nous limitant à l'état actuel des connaissances et des évolutions en la matière. Nous commencerons par définir ce qu'est le profilage au sens large et par délimiter le cadre de notre analyse, puis nous nous intéresserons plus particulièrement au développement du profilage publicitaire. Nous nous attellerons enfin à une analyse des principaux procédés mis en œuvre au cours des différentes étapes du profilage publicitaire. Ce chapitre sera l'occasion d'évoquer la manière dont Facebook l'emploie comme élément central et essentiel de son modèle économique et les problèmes que cela génère en matière de protection des données.

Section 1 : Du profilage au profilage publicitaire

§1. La place du profilage publicitaire au sein de la notion de profilage

La pratique du profilage correspond à un traitement de données personnelles qui tombe sous le régime du RGPD[202]. Le règlement définit le profilage comme « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique* »[203].

Avant de rentrer dans toute autre considération il est donc important de s'interroger sur le caractère personnel des données en question afin de savoir si la définition du profilage donnée par le

[201] A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 291.
[202] RGPD, cons. 72.
[203] *Ibid.*, art. 4, §4.

RGPD s'applique à un cas d'espèce[204]. Même si le profilage « *va bien souvent de pair avec le suivi des internautes* »[205], il reste possible qu'une analyse se base sur des données anonymisées et dans cette hypothèse le RGPD ne trouvera pas à s'appliquer. Toutefois comme nous l'avons évoqué précédemment, le fait qu'une donnée soit anonymisées n'assurant pas qu'elle le sera toujours, il serait imprudent de la part d'un responsable de traitement utilisant des données anonymisées d'éluder d'emblée l'application des précautions requises par le règlement[206].

Lorsque l'on est en présence de données personnelles, ou qui pourraient potentiellement le devenir, il faut ensuite vérifier que deux conditions soient rencontrées afin de déterminer si nous sommes confrontés à un cas de profilage. De manière simplifiée, la définition du règlement suppose « *quant aux moyens : une forme automatisée de traitement (intégralement ou partiellement)* »[207] et « *quant aux finalités : l'évaluation d'aspects personnels au sujet d'une personne physique* »[208]. Le profilage est un procédé de plus en plus répandu, et les moyens dédiés à sa mise en œuvre sont de plus en plus nombreux. Ils comprennent en effet « *une multitude de techniques sur la base de différentes technologies difficiles à appréhender et toujours en évolution* »[209]. Mais le profilage n'étant pas « *une finalité en soi* »[210], les objectifs qu'il rencontre sont presque tout aussi variés, et les « *modalités technique*s »[211] mises à sa disposition lui permettent d'atteindre divers objectifs « *dans de nombreux secteurs d'activités relevant du secteur public ou du secteur privé* »[212]. C'est pourquoi dans la pratique, il est plus complexe de le définir et de le délimiter[213].

En ce qui concerne les différentes finalités du profilage, il est intéressant de noter qu'il prend tout son sens lorsqu'il sert l'intérêt général. Le RGPD précise justement que « *le traitement des données à caractère personnel devrait être conçu pour servir l'humanité* »[214]. C'est le cas lorsqu'il

---

[204] J.-P. WALTER, *Le profilage des individus à l'heure du cyberespace: un défi pour le respect du droit à la protection des données*, 2009 (article en ligne disponible sur https://dokodoc.com/queue/le-profilage-des-individus-a-l-heure-du-cyberespace-un-defi-.html, dernière consultation le 06 août 2019), pp. 13-14.
[205] J.-F. PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *op. cit.*, p. 68.
[206] A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, p. 19.
[207] F. COTON et P. LIMBREE, « 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) », *op. cit.*, p. 23.
[208] *Ibid.*
[209] A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 291.
[210] J.-P. WALTER, *Le profilage des individus à l'heure du cyberespace: un défi pour le respect du droit à la protection des données* (en ligne), *op. cit.*, p. 8.
[211] *Ibid.*
[212] *Ibid.*, pp.16-17.
[213] A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 291.
[214] RGPD, cons. 4.

est utilisé par le pouvoir judiciaire et les autorités publique, pour éviter les fraudes par exemple[215]. Le fait de “profiler" les individus peut également présenter des avantages sociaux et culturels. Mais aux yeux de nombreuses entreprises, le profilage représente surtout un intérêt économique considérable. Initialement, le recours à cette pratique permettait notamment aux sites Internet de différentes marques « *de faciliter les sessions de l'utilisateur, en maintenant, par exemple, le panier d'achats ou les préférences de l'utilisateur* »[216]. Aujourd'hui, le recours au profilage est principalement utilisé par ces entreprises à des fins publicitaires : « *fidélisation des clients, localisation de clients potentiels, identification de clients susceptibles d'être intéressés par de nouveaux produits, offre privilégiée (modulation des prix en fonction du profil)* »[217]. Nous nous concentrons sur cet aspect du profilage.

§2. Le développement du profilage publicitaire

Le modèle économique de base des Géants d'Internet consiste à financer le fonctionnement de leurs plateformes en mettant des encarts à disposition des annonceurs publicitaires[218]. Les rétributions que ces annonceurs leur octroient à cette occasion permettent de proposer aux internautes des services qui restent gratuits. Cependant, les utilisateurs des plateformes ont commencé à réagir à cette invasion constante de publicités de nature aléatoire au cours de leur navigation, souvent en faisant usage d'extensions web telles qu'Adblock afin de les masquer[219]. Il était donc nécessaire, à la fois pour les plateformes et pour les annonceurs, de mettre en place un système permettant de diminuer la quantité de publicités présentées tout en les rendant plus pertinentes[220].

C'est pour cette raison que s'est développé le recours au profilage publicitaire, qui permet d'identifier les cibles idéales de chaque type de publicité[221]. Le modèle économique initial a donc évolué vers un accord entre les individus et les opérateurs qui « *se résume dans le consentement à*

---

[215] A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 280.
[216] *Ibid.*, p. 284
[217] J.-P. WALTER, *Le profilage des individus à l'heure du cyberespace: un défi pour le respect du droit à la protection des données* (en ligne), *op. cit.*, pp. 16-17.
[218] I. LANDREAU, L. LÉGER et V. PEZ-PÉRARD, « Partie 1 : Les aspects socio-économiques et éthiques des données personnelles », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles*, (Sous la direction de LÉGER L.), janvier 2018 (disponible sur https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf, dernière consultation le 06 août 2019), p. 26.
[219] *Ibid.*
[220] *Ibid.*
[221] *Ibid.*

l'exploitation commerciale – au sens large – de données à caractère personnel en échange du service offert »[222]. Il ne s'agit pas pour autant d'un « *transfert de propriété* »[223] mais plutôt d'un droit d'accès mutuel : l'accès à la plateforme par les utilisateurs en échange de l'accès aux données de ces utilisateurs par la plateforme. Cet échange de bons procédés est parfois appelé pacte Softien, qui correspond à une contraction entre "*software*" et "pacte faustien"[224], plus communément appelé pacte avec le diable[225].

Dès lors, les utilisateurs assidus et réguliers représentent des cibles particulièrement intéressantes[226] puisque la quantité d'informations privées qu'ils partagent « *offrent un marché précis aux publicitaires souhaitant diffuser des publicités ciblées* »[227]. Au plus le profilage est spécifique, au plus les annonceurs publicitaires rentabilisent leur investissement puisque cela leur permet d'améliorer « *le ratio entre le nombre d'individus qui ont réellement adopté le comportement souhaité, comme acheter le produit par exemple, sur le nombre de publicités jouées/ payées par l'annonceur* »[228]. Les données sont ainsi devenues « *une source de revenus considérable, via l'augmentation de la valeur des espaces publicitaires vendus (du fait d'un meilleur ciblage possible), et la revente aux "partenaires"*»[229].

Section 2 : Les étapes du profilage publicitaire

Le profilage comprend trois temps distincts. Le processus commence par une « *collecte à grande échelle de données personnelles* »[230]. Ces données sont ensuite analysées[231]. C'est au terme de cette étape que les individus se voient appliquer un profil[232], ce qui entraîne des « *sollicitations, par affichage d'encarts publicitaires sur Internet, envoi d'e-mails ou simples envois postaux* »[233].

---

[222] J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, p. 241.
[223] Y. POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.*, pp. 29-30.
[224] G. KOENIG, « Introduction », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles* (en ligne), *op. cit.*, p. 14.
[225] Le Petit Larousse illustré grand format, édition 2013.
[226] Avis n° 5/2009 du Groupe de Travail de l'Article 29 sur les réseaux sociaux en ligne, WP 163, 12 juin 2009 (01189/09/FR), p. 5.
[227] *Ibid.*
[228] I. LANDREAU, L. LÉGER et V. PEZ-PÉRARD, « Partie 1 : Les aspects socio-économiques et éthiques des données personnelles », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles* (en ligne), *op. cit.*, p. 31.
[229] *Ibid.*, p. 27.
[230] A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, pp. 291-292.
[231] *Ibid.*
[232] *Ibid.*
[233] J.-F. PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *op. cit.*, p. 67.

Ces différentes étapes impliquent diverses techniques et de nombreux concepts, mais soulèvent surtout plusieurs problèmes en matière de protection des données.

§1. La collecte

A. Les types de profils à composer

L'objectif de la collecte effectuée par Facebook est de réunir différentes sortes d'informations destinées à composer un profil de l'internaute. Le terme de "profil" sur un réseau social est double[234]. Il faut en différencier deux types, que la CNIL (APD française) nomme "profil explicite" et "profil prédictif"[235]. Le profil explicite correspond aux informations renseignées par l'utilisateur de manière volontaire[236], que ce soit « *en s'inscrivant sur un service en ligne ou en les publiant sur un réseau social* »[237]. Le profil prédictif est basé sur l'observation à long terme de son comportement[238], « *par exemple en suivant et analysant les actions de l'internaute au travers de ces différents clics (page visitée, mots clés, production de contenu en ligne, etc)* »[239].

Certains considèrent que le profil prédictif, composé des données rassemblées principalement par ces outils, n'est qu'une extension du profil explicite à laquelle l'utilisateur n'a pas accès[240]. Mais un profil prédictif peut également exister indépendamment de tout profil explicite, ce qui signifie qu'il n'est pas nécessaire de remplir un quelconque formulaire ou de fournir des indications de notre plein gré pour faire l'objet de profilage publicitaire[241]. Nous pouvons en déduire qu'il est impossible pour un internaute de rester totalement anonyme puisque les données récoltées tout au long de sa navigation permettent de le rendre identifiable[242] au sens du RGPD. Cela pose déjà des

---

234 J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, p. 236.
235 A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 293.
236 Site officiel de la CNIL, *La publicité ciblée en ligne, communication présentée en séance plénière*, le 5 février 2009 (article en ligne disponible sur https://www.cnil.fr/sites/default/files/typo/document/Publicite_Ciblee_rapport_VD.pdf, dernière consultation le 06 août 2019), p.11.
237 J.-P. WALTER, *Le profilage des individus à l'heure du cyberespace: un défi pour le respect du droit à la protection des données* (en ligne), *op. cit.*, p. 10.
238 Site officiel de la CNIL, *La publicité ciblée en ligne, communication présentée en séance plénière*, (en ligne), *op. cit.*, p.11.
239 J.-P. WALTER, *Le profilage des individus à l'heure du cyberespace: un défi pour le respect du droit à la protection des données* (en ligne), *op. cit.*, p. 9.
240 J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, p. 236.
241 I. LANDREAU, L. LÉGER et V. PEZ-PÉRARD, « Partie 1 : Les aspects socio-économiques et éthiques des données personnelles », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles* (en ligne), *op. cit.*, p. 26.
242 J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, p. 242.

questions en matière de consentement[243] et de transparence[244] puisque cette démarche a souvent lieu à l'insu des individus.

B. Les principaux outils d'identification en ligne

Selon le Groupe de Travail de l'Article 29, il n'est même pas requis de connaitre le nom de quelqu'un pour lui attribuer un profil sur Internet : une "adresse IP" ou un "cookie de navigation" avec un identifiant unique suffit[245]. Le RGPD reconnaît aussi la capacité d'identification que ces outils représentent de par leur tendance à « *laisser des traces* »[246].

Une adresse IP est un identifiant unique exploité par le « *protocole de routage de l'Internet qu'on pourrait qualifier d'adresse sur le réseau* »[247]. Elle est soit dynamique, soit permanente[248]. Le fait de récolter les adresses IP ayant consulté un site Internet constitue un traitement de données personnelles, même en cas d'adresse IP dynamique si la combinaison de celle-ci avec d'autres informations permet d'identifier son propriétaire[249].

Quant au recours à des cookies de navigation, il s'agit d'une manière classique de suivre le comportement des individus en ligne. Un cookie correspond à un « *petit morceau de texte généré par un serveur Web* »[250] qui fait office de « *témoin* »[251]. Il est intégré au navigateur d'un internaute lorsque celui-ci visite un site et permet au serveur ayant généré ce cookie d'enregistrer et de tracer ses activités[252] : « *les pages visitées, le parcours suivi, le temps passé par page, les produits visualisés, les informations lues, les produits mis au panier, les produits réellement achetés, etc.* »[253]. Deux types de cookies sont à distinguer : les cookies temporaires et les cookies persistants. Les

---

243 RGPD, art. 6, §1, a).
244 RGPD, art. 5, §1, a).
245 Avis n° 1/2008 du Groupe de Travail de l'Article 29 sur les aspects de la protection des données liés aux moteurs de recherche, WP 148, 4 avril 2008 (00737/FR), p. 9.
246 RGPD, cons. 30.
247 L. PAILLER, « Chapitre 1 - L'affaiblissement de la vie privée personnelle par le réseau social », *in Les réseaux sociaux sur internet et le droit au respect de la vie privée*, Bruxelles, Larcier, 2012, pp. 115-116.
248 *Ibid.*
249 C. GAYREL, « Chapitre 12. - L'expansion des standards européens de protection des données dans le monde » *op. cit.*, p. 479.
250 A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 287.
251 J.-F. PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *op. cit.*, p. 67.
252 A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 287.
253 I. LANDREAU, L. LÉGER et V. PEZ-PÉRARD, « Partie 1 : Les aspects socio-économiques et éthiques des données personnelles », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles* (en ligne), *op. cit.*, p. 31.

cookies temporaires sont propres à la session en cours et permettent d'enregistrer les choix effectués par l'internaute sur un site[254]. Les cookies persistants contiennent un « *identifiant unique* »[255] et « *restent sur l'ordinateur tant qu'ils ne sont pas supprimés* »[256]. Le caractère de ceux-ci peut aller de « *très peu intrusifs et utiles (retenir la langue choisie sur un site par ex.) à excessivement intrusifs* »[257] lorsqu'ils permettent d'enregistrer le parcours de la navigation et de stocker une quantité beaucoup plus importante d'informations[258]. Le cookie devient alors un véritable « *logiciel espion* »[259]. Les informations qu'ils recueillent permettent entre autres de compléter les données disponibles via les adresses IP. L'installation d'un cookie dans le navigateur d'un utilisateur aux fins de stockage des informations concernant son comportement ne constitue pas un traitement de données personnelles[260], cela consiste simplement en une « *étape préparatoire* »[261]. C'est l'accès à ces informations qui implique un traitement de données[262], et qui doit dès lors être soumis aux règles du RGPD.

Facebook utilise les adresses IP de ses utilisateurs, entre autres afin de déterminer leur géolocalisation[263]. Le réseau social fait également usage de la technologie des cookies de navigation via son site Internet mais aussi au travers des "plug-ins sociaux" (boutons "j'aime", "commenter", "se connecter"…[264]) installés sur des sites tiers[265]. La C.J.U.E. a d'ailleurs décidé que ces sites tiers disposant de tels modules étaient désormais dans l'obligation d'informer leurs visiteurs de la transmission de ces données au fournisseur du module, en l'occurrence Facebook[266].

---

254 A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 287.
255 Avis n° 1/2008 du Groupe de Travail de l'Article 29 sur les aspects de la protection des données liés aux moteurs de recherche, WP 148, 4 avril 2008 (00737/FR), p. 9.
256 A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 287.
257 J.-F. PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *op. cit.*, p. 67.
258 A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 287.
259 E. DEGRAVE, *Facebook, les cookies et la justice belge : le retour* (en ligne)*, op. cit.*
260 Directive (CE) n° 58/2002 du Parlement européen et du Conseil du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *J.O.C.E.*, L 201, du 31 juillet 2002, p. 037, art. 5, § 3.
261 J.-F. PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *op. cit.*, p. 67.
262 *Ibid.*, p. 68.
263 J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, p. 238.
264 B. BATHELOT, *Définition : Plugins sociaux Facebook*, Définitions Marketing, le 25 juillet 2015 (article en ligne disponible sur https://www.definitions-marketing.com/definition/plugins-sociaux-facebook/, dernière consultation le 06 août 2019).
265 E. DEGRAVE, *Facebook, les cookies et la justice belge : le retour* (en ligne)*, op. cit.*
266 Arrêt Fashion ID GmbH & Co. KG/Verbraucherzentrale NRW eV, C-40/17, EU:C:2019:629, pt. 106.

Dans l'affaire que nous avons évoquée dans le cadre du premier chapitre, et qui fait actuellement l'objet d'une question préjudicielle à la C.J.U.E., la CPVP reproche à Facebook le traçage des internautes effectué par Facebook à leur insu[267]. En effet l'entreprise possède une quantité importante de données concernant ses utilisateurs, mais aussi d'individus n'ayant aucun compte sur le réseau social, et ce toujours à leur insu[268]. C'est le cookie Datr qui permet à Facebook d'étendre à ce point sa récolte de données, puisqu'il s'installe automatiquement sur le navigateur de tout internaute dès lors que celui-ci visite le réseau social, peu importe qu'il soit inscrit ou non[269]. Ce cookie permet de tracer sa navigation au fil d'autres sites comportant un plug-in social relatif à Facebook[270]. Ceux-ci, dans l'autre sens, « *communiquent à Facebook, via les cookies, des informations, parfois sensibles, au sujet des utilisateurs du web* »[271].

Toutefois, ces techniques ne sont pas les seuls moyens utilisés par Facebook pour collecter des données personnelles. Il existe d'autres outils informatiques permettant d'analyser le comportement des internautes. Qui plus est, les individus fournissent parfois des informations sur eux-mêmes sans réellement s'en rendre compte. À titre d'exemple, nous citerons l'application *Rewards* de Facebook, qui a proposé en 2017 à ses utilisateurs une fonctionnalité[272] permettant « *de scanner des QR codes déployés en magasins physiques pour bénéficier de promotions ciblées* »[273]. Cette possibilité d'obtenir des promotions du simple fait d'être inscrit sur Facebook représentait aussi un moyen pour les magasins de faire varier leur clientèle[274], mais permettait surtout à Facebook de collecter toujours plus d'informations sur ses membres[275], en l'occurrence sur leurs habitudes d'achats.

---

267 Civ. Bruxelles nl. (réf.), 9 novembre 2015, *J.L.M.B.*, 2017, liv. 26, p. 1240.
268 J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, p. 242.
269 T. DERIDDER, *Affaire APD contre Facebook – la CJUE saisie !* (en ligne), *op. cit.*
270 *Ibid.*
271 G. DEJEMEPPE, « L'affaire Facebook : questions de procédure », *R.D.T.I.*, 2016/1, n° 62, p. 113.
272 I. LANDREAU, L. LÉGER et V. PEZ-PÉRARD, « Partie 1 : Les aspects socio-économiques et éthiques des données personnelles », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles* (en ligne), *op. cit.*, p. 30.
273 *Ibid.*
274 J. CONSTINE, *'Facebook Rewards' QR codes dangle discounts for offline purchases*, Techcrunch, 2017 (article en ligne disponible sur https://techcrunch.com/2017/05/01/facebook-rewards/, dernière consultation le 06 août 2019).
275 I. LANDREAU, L. LÉGER et V. PEZ-PÉRARD, « Partie 1 : Les aspects socio-économiques et éthiques des données personnelles », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles* (en ligne), *op. cit.*, p. 30.

C. Le concept de Big Data

Il est impossible de définir précisément le Big Data, et le RGPD n'a même pas tenté de le faire[276] alors que les données concernées par le Big Data sont souvent des données personnelles[277]. De manière générale, la notion de Big Data correspond à la « *pratique qui consiste à combiner d'énormes volumes d'informations provenant de différentes sources et à les analyser en utilisant des algorithmes plus complexes pour mieux étayer les décisions* »[278]. Elle représente donc une opportunité de sonder l'amas de données généré principalement par les outils que nous avons évoqués, mais aussi celles renseignées par les individus eux-mêmes. Les caractéristiques spécifiques au Big Data permettent de mieux comprendre ce qu'il implique[279]. Il est d'usage de parler des 3V, qui se réfèrent à un grand Volume, une grande Vélocité et une grande Variété, auxquels peuvent être ajoutés la Valeur et la Véracité[280].

Le Volume désigne une volonté de maximiser la quantité de données collectées. La « *capacité accrue de la technologie à supporter la collecte et le stockage de grandes quantités de données* »[281], le « *faible coût de conservation de ces données* »[282] et le fait que cela se passe « *sans que les personnes auxquelles elles ont trait en aient conscience* »[283] sont des facteurs qui encouragent ce phénomène. Pourtant, celui-ci va à l'encontre du principe de minimisation des données imposé par le RGPD, qui requiert que les données collectées soient « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* »[284].

La Vélocité évoque la vitesse à laquelle cet ensemble de données est produit et analysé[285]. Une grande proportion de ces données étant « *générée automatiquement* »[286], le processus a lieu à une

---

276 F. COTON et P. LIMBREE, « 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) », *op. cit.*, p. 10.
277 A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, pp. 15-16.
278 Avis n° 7/2015 du Contrôleur européen de la protection des données sur les défis des données massives, 19 novembre 2015 p. 8.
279 A. STROWEL, « Mutations des propriétés intellectuelles et du droit d'auteur à l'ère des données (data ownership, text and data mining, hyperlinking) », *A&M*, 2017/4, p. 320.
280 *Ibid.*
281 Avis n° 7/2015 du Contrôleur européen de la protection des données sur les défis des données massives, 19 novembre 2015 p..8.
282 F. COTON et P. LIMBREE, « 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) », *op. cit.*, pp. 10-11.
283 *Ibid.*
284 RGPD, art. 5, §1, c).
285 F. COTON et P. LIMBREE, « 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) », *op. cit.*, pp. 10-11.
286 *Ibid.*

rapidité impressionnante. Elles sont également « *analysées en profondeur et traitées rapidement, idéalement en temps réel, par des algorithmes informatiques* »[287].

La Variété signifie que des données de tous types sont rassemblées, sans égard pour leur source ou leur format[288], et sont souvent « *non structurées* »[289]. Cependant il a fallu attendre « *les développements de l'intelligence artificielle et des outils d'analyse de donnée*s »[290] pour pouvoir exploiter efficacement cette masse jusque-là indéchiffrable. Le développement des technologies permet désormais de déduire de nombreuses informations[291] sur base des données « *a priori sans valeur particulière* »[292], qui étaient parfois même conservée sans raison définie[293].

L'ajout du critère de Valeur a justement trait à cette capacité qu'a le Big Data de « *valoriser la masse parfois insoupçonnée de données contenues dans leurs serveurs* »[294]. Prises séparément, ces données sont sans intérêt, mais une fois qu'il est possible de les comparer ou de les combiner à d'autres données, elles prennent de la valeur[295] puisqu'elles permettent notamment d'identifier le « *comportement d'un profil social* »[296]. C'est, en effet la volonté de tirer profit des données dont elles disposent qui a encouragé tant d'entreprises à recourir au principe du Big Data[297]. Facebook en est un exemple typique[298].

En ce qui concerne le critère de Véracité, il n'est pas aussi pertinent que les autres puisque les données collectées n'ont pas besoin d'être vraies pour être inclues dans une collecte de type Big

---

[287] A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 290.
[288] F. COTON et P. LIMBREE, « 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) », *op. cit.*, pp. 10-11.
[289] A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 290.
[290] F. COTON et P. LIMBREE, « 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) », *op. cit.*, pp. 10-11.
[291] A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, p. 15.
[292] *Ibid.*
[293] *Ibid.*
[294] *Ibid.*
[295] N. BINCTIN, « Partie 2 : Créer une patrimonialité des données à droit constant », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles* (en ligne)*, op. cit.*, p. 53.
[296] *Ibid.*
[297] A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, p. 15.
[298] Facebook Research, *Facebook's Top Open Data Problems*, by J. WIENER and N. BRONSON, le 22 octobre 2014 (article disponible sur https://research.fb.com/blog/2014/10/facebook-s-top-open-data-problems/, dernière consultation le 06 août 2019).

Data. Cependant, le RGPD impose de n'utiliser que des données « *exactes et, si nécessaire, tenues à jour* »[299], dans la mesure du possible[300]. Il serait donc préférable que ce critère soit rencontré.

D. L'anonymisation et la pseudonymisation

Au terme de la collecte, il est possible de dépasser le fait que les données rassemblées soient majoritairement relatives à des individus[301] et les problèmes que cela implique en matière de protection des données personnelles et surtout de vie privée, et ce grâce aux techniques d'anonymisation et de pseudonymisation des données rassemblées.

L'anonymisation consiste à « *supprimer les éléments directement identifiants et quasi identifiants (permettant en les recoupant avec d'autres données de réidentifier une personne)* »[302]. Le RGPD ne s'appliquera donc plus au traitement de ces données[303], puisqu'elles ne peuvent plus « *être rattachées à une personne individualisée* »[304]. Attention toutefois au fait que la manipulation des données à des fins d'anonymisation constitue un traitement de données personnelles[305].

Cependant, l'anonymisation pose deux problèmes majeurs. Premièrement, cette technique représente de moins en moins une sécurité en matière de protection des données puisque comme nous l'avons évoqué dans le premier chapitre, l'accès à une quantité de données exponentielle et l'évolution des techniques sont des facteurs qui impliquent des risques de plus en plus élevés de réidentification des données[306]. Les concepts d'anonymisation et de réidentification sont effectivement devenus « *des domaines de recherche très actifs présentant des avancées technologiques constantes* »[307]. Il est donc de moins en moins possible d'avoir affaire à des données réellement anonymes[308]. Deuxièmement, cette technique consistant en une modification ou une généralisation des données réduit leur qualité, parfois jusqu'à leur ôter tout intérêt[309].

---

[299] RGPD, art. 5, §1, d).
[300] *Ibid.*, art. 5, §1, d).
[301] A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, pp. 15-16.
[302] *Ibid.*, p. 19.
[303] RGPD, cons. 26.
[304] A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 296.
[305] F. COTON et P. LIMBREE, « 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) », *op. cit.*, p. 15.
[306] A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, p. 19.
[307] A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 297.
[308] A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, pp. 18-19.
[309] *Ibid.*

La pseudonymisation, dont la pratique ne soustrait pas les données au champ d'application du RGPD, consiste en une transformation des données personnelles en données chiffrées. Le règlement le définit comme un « *traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable* »[310]. Cette technique est un moyen de « *réduire les risques pour les personnes concernées et aider les responsables du traitement et les sous-traitants à remplir leurs obligations en matière de protection des données* »[311].

§2. L'analyse

« *The data warehouse provides the enterprise with a memory. But memory is of little use without intelligence* »[312].

La conservation des données rassemblées représente une mémoire, et les outils et techniques que regroupent le principe de forage de données (ou *data mining*) permettent d'ajouter de l'intelligence à cette mémoire[313]. Ce principe consiste en « *l'application des techniques statistiques, d'analyse de données et d'intelligence artificielle à l'exploration et à l'analyse dans a priori de (souvent grandes) bases de données informatiques, en vue d'extraire des informations nouvelles et utiles pour le détenteur de ces données* »[314].

Sur base de cette masse de données diverses augmentant sans cesse, il est donc possible de déduire des informations. Non pas au travers d'un « *principe de causation (le know why)* »[315] mais bien dans le but de « *saisir des corrélations (le know what)* »[316]. En d'autres mots, il ne s'agit pas

---

[310] RGPD, art. 4, §5.
[311] *Ibid.*, cons. 28.
[312] M. BERRY et G. LINOFF, *Data Mining Techniques: For Marketing, Sales, and Customer Relationship Management (second edition)*, Indianapolis, Wiley Publishing Inc, 2004, pp. 5-6.
[313] *Ibid.*
[314] S. TUFFERY, *Data mining et statistique décisionnelle, l'intelligence dans les bases de données*, Paris, Technip, 2010, p. VII.
[315] A. STROWEL, « Mutations des propriétés intellectuelles et du droit d'auteur à l'ère des données (data ownership, text and data mining, hyperlinking) », *op. cit.*, p. 320.
[316] *Ibid.*

de comprendre l'origine ou l'explication des informations contenues dans ces données mais plutôt de déceler des symétries entre les jeux de données afin d'en déduire d'autres informations.

Ces données sont de ce fait rassemblées et analysées « *pour voir ce qu'on pourrait en tirer plutôt que pour aboutir à un résultat déterminé* »[317]. Cette optique va totalement à l'encontre du principe de limitation des finalité repris dans le RGPD, qui impose que les données personnelles soient « *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités* »[318].

Le résultat potentiel est obtenu au moyen d'un algorithme, qui consiste en « *une série ordonnée d'étapes univoques exécutables décrivant un processus fini, en d'autres mots, d'une série d'instructions élémentaires qui s'enchaînent selon des règles précises, sans place pour l'interprétation personnelle* »[319]. L'intérêt d'un algorithme est justement de pouvoir « *ordonner ou filtrer des données, établir des calculs statistiques ou regrouper des données par affinités* »[320] via des procédés automatisés. C'est ce qui permet de constituer des profils sur base de données personnelles.

§3. L'application d'un profil

A. Les types de profilages publicitaires

Selon le Groupe de Travail de l'Article 29, il existe différents types de procédés permettant aux marques d'atteindre les internautes via les réseaux sociaux. Le plus évident est le marketing segmenté qui consiste à répartir les utilisateurs d'un réseau social en différentes catégories sur base des informations qu'ils mettent à disposition et à leur présenter des publicités susceptibles d'intéresser cette catégorie de personnes[321]. Le marketing contextuel quant à lui est « *adapté au contenu que l'utilisateur voit ou auquel il accède* »[322]. Cela correspond à la situation dans laquelle

---

317 F. COTON et P. LIMBREE, « 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) », *op. cit.*, p. 30.
318 RGPD, art. 5, §1, b).
319 F. COTON et P. LIMBREE, « 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) », *op. cit.*, p. 11.
320 A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 292.
321 Avis n° 5/2009 du Groupe de Travail de l'Article 29 sur les réseaux sociaux en ligne, WP 163, 12 juin 2009 (01189/09/FR), p. 5.
322 *Ibid.*

un internaute effectue une recherche sur le site d'une agence de voyage et se voit proposer presqu'instantanément sur Facebook des publicités pour des vols en avion et des hôtels en tous genres. Le troisième, le marketing comportemental, est le plus intrusif puisqu'il sélectionne les publicités par l'observation et l'analyse des activités de l'utilisateur[323].

Ces différentes stratégies marketing permettent d'identifier deux grandes sortes de profilage : le profilage spécifique et le profilage abstrait.

Le profilage spécifique (ou individuel) se base uniquement sur « *l'assemblage de données "appartenant" à la personne* »[324], qui est issu de la collecte et l'analyse de ces données[325]. Le marketing contextuel, qui utilise à ces fins le profil prédictif d'un internaute, est basé sur ce genre de profilage.

Le profilage abstrait (ou de groupe) repose sur des données qui ne sont pas uniquement celles de la personne visée[326], qu'il s'agisse uniquement de son profil explicite, de son profil explicite augmenté d'un profil prédictif, ou de son seul profil prédictif. Ce processus, qui repose sur une stratégie Big Data, commence par la récolte de données personnelles, qui seront ou non anonymisées[327] ou pseudonymisées, dans le but d'observer les « *caractéristiques d'individus qui n'ont pas besoin d'être identifiés ou identifiables* »[328]. Il faut ensuite, au moyen du forage de données[329], identifier « *un lien de probabilités entre certains comportements ou certaines caractéristiques et d'autres comportements ou caractéristiques* »[330]. L'objectif de la démarche est de parvenir à créer un groupe d'individus selon leurs caractéristiques communes, puis de déduire de leurs caractéristiques individuelles d'autres caractéristiques susceptibles de s'appliquer à l'ensemble du groupe[331]. Au terme de ce type de profilage, une personne se verra appliquer un profil issu de la

---

323 Avis n° 5/2009 du Groupe de Travail de l'Article 29 sur les réseaux sociaux en ligne, WP 163, 12 juin 2009 (01189/09/FR), p. 5.
324 J.-P. WALTER, *Le profilage des individus à l'heure du cyberespace: un défi pour le respect du droit à la protection des données* (en ligne), *op. cit.*, p. 8.
325 A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 292.
326 J.-P. WALTER, *Le profilage des individus à l'heure du cyberespace: un défi pour le respect du droit à la protection des données* (en ligne), *op. cit.*, p. 8.
327 A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 292.
328 *Ibid.*
329 *Ibid.*
330 J.-P. WALTER, *Le profilage des individus à l'heure du cyberespace: un défi pour le respect du droit à la protection des données* (en ligne), *op. cit.*, p. 8.
331 A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 292.

comparaison entre ses données et un « *profil de référence* »[332] ou basé sur l'association de ses données à celles d'un groupe par inférence[333]. Le marketing segmenté est par définition une application du profilage abstrait (ou de groupe), qui se limite toutefois à analyser le profil explicite des individus.

Le marketing comportemental est également une pratique issue du profilage abstrait, mais qui va agir de manière beaucoup plus pernicieuse que le marketing segmenté. Il exploite le profil explicite d'un utilisateur augmenté de son profil prédictif, ou même uniquement son profil prédictif afin de produire un troisième type de profil. Celui-ci représente en quelque sorte la manière dont les algorithmes définissent les individus[334]. De manière imagée, cela consiste en un « *reflet numérique* »[335] de chacun, permettant d'identifier précisément les « *besoins d'un point de vue publicitaire* »[336].

L'évolution des technologies est telle qu'elles octroient à un ensemble de données analysées un « *pouvoir de déduction* »[337] impressionnant, de par les « *renseignements sans précédent sur le comportement humain, la vie privée de chacun et nos sociétés* »[338] qu'elles sont désormais capables de fournir.

Il ressort de ce qui précède que le profil final d'une personne constitué par une stratégie Big data « *n'est pas le résultat d'une construction autonome de la personne* »[339] puisqu'il est partiellement définit par les algorithmes, c'est à dire de manière automatisée[340]. De plus, les données personnelles sont nécessaires pour pouvoir les comparer à d'autres jeux de données, mais sont inutiles individuellement : ce qui compte, c'est le résultat des combinaisons des critères révélés

---

[332] J.-P. WALTER, *Le profilage des individus à l'heure du cyberespace: un défi pour le respect du droit à la protection des données* (en ligne), *op. cit.*, p. 8.
[333] *Ibid.*
[334] K. SZYMIELEWICZ, *Your digital identity has three layers, and you can only protect one of them*, Quartz, le 25 janvier 2019 (article en ligne disponible sur https://qz.com/1525661/your-digital-identity-has-three-layers-and-you-can-only-protect-one-of-them/, dernière consultation le 06 août 2019).
[335] D.-J. RAHMIL, *Vous ne contrôlez qu'un tiers de votre identité en ligne*, L'ADN, le 13 février 2019 (article en ligne disponible sur https://www.ladn.eu/tech-a-suivre/data-comment-construit-identite-ligne/, dernière consultation le 06 août 2019).
[336] *Ibid.*
[337] F. COTON et P. LIMBREE, « 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) », *op. cit.*, p. 11.
[338] *Ibid.*
[339] J.-P. WALTER, *Le profilage des individus à l'heure du cyberespace: un défi pour le respect du droit à la protection des données* (en ligne), *op. cit.*, p. 6.
[340] *Ibid.*

par les données de nombreuses personnes qui détermine le profil d'un individu[341]. C'est pour ces raisons qu'on peut parler « *d'une construction d'identité hétéronome* »[342].

B. Le *Modus Operandi* entre Facebook et les annonceurs publicitaires

Facebook, qui utilise une stratégie Big Data et combine le profilage spécifique et le profilage abstrait, est en mesure de fournir à ses annonceurs « *de multiples ciblages démographiques, géographiques, linguistiques, en fonction des intérêts voire en fonction des personnes avec lesquels le public ciblé est "ami"* »[343]. Via Facebook Business, Facebook propose aux marques de choisir l'orientation de leurs campagnes et de définir leur audience[344] grâce à des combinaisons de ces différents "ciblages". Il se charge ensuite lui-même « *d'afficher la publicité sur les pages des internautes concernés* »[345]. Il s'agit d'un cas de « *publicité sur site* »[346], « *dont la diffusion est contrôlée par Facebook qui indique qu'aucune donnée personnelle n'est transmise aux annonceurs* »[347]. Nous pouvons donc en déduire que Facebook conserve précieusement ses bases de données.

Il existe un autre système, qui consiste pour un site internet à passer par une « *régie publicitaire* »[348]. Dans ce cas, c'est un tiers qui collecte les informations des internautes au fil de leurs visites sur différents sites dépendant de la même régie[349]. Ce tiers propose aux annonceurs des critères de ciblage pour leurs publicité et affichera lui-même la publicité sur l'interface de tous ces sites[350]. Une régie fait office de « *fournisseur de réseaux publicitaires* »[351].

Il ne fait aucun doute que l'option choisie par Facebook pour l'affichage des publicités sur son interface correspond à un cas de publicité sur site. Cependant, il est pertinent de se demander si

---

341 Y. POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.*, p. 29.
342 J.-P. WALTER, *Le profilage des individus à l'heure du cyberespace: un défi pour le respect du droit à la protection des données* (en ligne), *op. cit.*, p. 6.
343 L. PAILLER, « Chapitre 1 - L'affaiblissement de la vie privée personnelle par le réseau social », *op. cit.,* pp. 112-113.
344 Facebook Business, *Publicités Facebook, Entrez en contact avec de futurs clients et fans* (disponible sur https://www.facebook.com/business/ads, dernière consultation le 06 août 2019).
345 A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 283.
346 Site officiel de la CNIL, *La publicité ciblée en ligne, communication présentée en séance plénière*, (en ligne), *op. cit.*, p. 6.
347 *Ibid.*, p. 15.
348 *Ibid.*, p. 6.
349 *Ibid.*
350 *Ibid.*, p. 6.
351 A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 288.

l'entreprise n'agit pas elle-même en quelque sorte comme une régie publicitaire[352] au travers de ses plug-ins éparpillés sur la toile. Si elle ne fait que mettre à disposition des critères permettant à des tiers d'atteindre un public cible, ce n'est pas le cas, mais si Facebook propose à des tiers spécifiques d'atteindre tel ou tel public qu'il définit, créant ainsi la demande, la question se pose.

Section 3 : Les dérives du profilage publicitaire

Nous avons observé de nombreux problèmes que pose le profilage publicitaire en termes de protection des données personnelles, qui impliquent que certaines règles doivent être respectées. Nous traiterons de celles-ci dans le cadre du dernier chapitre. Cependant, l'utilisation de ces données, destinées initialement au profilage publicitaire, peut comporter des risques de dérives autrement préoccupants.

Tout d'abord, le profilage peut mener à des discriminations ou à des exclusions[353], en ne proposant certaines publicités qu'à certaines catégories de personnes par exemple.

Par ailleurs, certaines expériences ont été mises en place par Facebook à l'insu de ses utilisateurs, qui consistaient à observer les réactions émotionnelles des individus face à des modifications de l'interface ou des publications proposées dans leur fil d'actualité[354]. Le réseau social s'est prévalu pour sa défense de « *termes contractuels l'autorisant à effectuer des "recherches et analyses" à partir des données collectées* »[355]. On observe surtout au travers de ce genre de cas que les GAFA ont tendance à chercher comment « *utiliser les données en s'appuyant sur les neurosciences pour pouvoir justement un peu aussi nous manipuler* »[356]. Cela laisse supposer que Facebook est aussi capable d'identifier les situations dans lesquelles les individus sont les plus vulnérables, ce qui permet d'amener le profilage publicitaire à un niveau supérieur : il est

---

[352] M. LE GUENNO, *Facebook étend sa régie publicitaire à tout le Web, y compris les non-membres*, Influenth, le 28 mai 2016 (article en ligne disponible sur http://www.influenth.com/facebook-regie-publicitaire/, dernière consultation le 06 août 2019).
[353] A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 280.
[354] G. KOENIG, « Introduction », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles* (en ligne), *op. cit.*, p. 13.
[355] *Ibid.*
[356] C. FRATI, *Le RGPD a une génération de retard,* interview de Cyril PIERRE-BEAUSSE (en ligne), *op. cit*.

envisageable que les publicités ciblées les incitent à effectuer des achats auxquels ils n'auraient peut-être pas pensé par eux-mêmes[357].

Toutefois, le profilage peut avoir des effets dont les conséquences sont d'une gravité qui atteint une bien plus grande échelle. Lorsqu'il touche aux « *campagnes politiques* »[358] par exemple. Dans le cadre du *Brexit*, Facebook a orienté les publications affichées en fonction de l'opinion des individus sur la question[359]. Cette démarche a eu une influence sur le résultat final[360] et « *c'est véritablement le fonctionnement démocratique qui en a été remis en cause* »[361].

La problématique en jeu dans l'affaire Cambridge Analytica est de même nature. Les données de millions d'utilisateurs de Facebook ont été extraites par l'entreprise Cambridge Analytica afin de manipuler les résultats de la campagne électorale de Donald Trump[362]. Elle a atteint un total de quatre-vingt-sept millions d'utilisateurs à travers le monde au moyen d'une application comportant un formulaire en ligne[363] en passant par une « *interface mise à disposition des développeurs tiers leur permettant d'interroger la base de données de Facebook des relations entre les utilisateurs* »[364]. Ce formulaire proposait de rémunérer les utilisateurs pour ce qui paraissait être un test de personnalité et demandait l'accès à leurs données personnelles, afin de compléter une étude académique[365]. Cette démarche, qui n'a été suivie en réalité que par un nombre limité de personne, a ouvert l'accès à leurs listes d'amis et aux données de ces amis[366]. Cambridge Analytica opérait en collaboration avec la campagne électorale de Donald Trump[367], et le rassemblement de ces données,

---

357 V. FOSSOUL, « L'identification par radiofréquence (RFID) : reflet des nouvelles tendances en matière de protection des données à caractère personnel », *in Le droit des nouvelles technologies et de l'internet*, Bruxelles, Bruylant, 2012, p. 128.

358 F. COTON et P. LIMBREE, « 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) », *op. cit.*, p. 11.

359 C. DE TERWANGNE, « Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel », *in L'Europe des droits de l'homme à l'heure d'Internet*, Bruxelles, Bruylant, 2019, p. 333.

360 *Ibid.*

361 *Ibid.*

362 C. FRATI, *Le RGPD a une génération de retard,* interview de Cyril PIERRE-BEAUSSE (en ligne), *op. cit*.

363 Royal Courts of Justice, Londres, 17 avril 2019, (disponible sur https://www.droit-technologie.org/wp-content/uploads/2019/05/954.pdf, dernière consultation le 06 août 2019) pt.2.

364 Site officiel de la CNIL, *Affaire Cambridge Analytica / Facebook*, le 12 avril 2018 (article en ligne disponible sur https://www.cnil.fr/fr/affaire-cambridge-analytica-facebook, dernière consultation le 06 août 2019).

365 C. CADWALLADR et E. GRAHAM-HARRISON, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, The Guardian, le 17 mars 2018 (article en ligne disponible sur https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election, dernière consultation le 06 août 2019).

366 Royal Courts of Justice, Londres, 17 avril 2019, (disponible sur https://www.droit-technologie.org/wp-content/uploads/2019/05/954.pdf, dernière consultation le 06 août 2019) pt.2.

367 C. CADWALLADR et E. GRAHAM-HARRISON, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, (en ligne), *op. cit.*

concernant en grande partie des américains[368], a permis d'identifier les individus susceptibles de changer d'avis quant à leur vote[369] et d'utiliser ces informations afin de faire de la « *prospection politique* »[370], à dessein de les manipuler. Il s'agit donc ici d'un problème de loyauté envers les personnes concernées[371], et par extension d'un problème de transparence[372].

De plus, comme nous l'avons exprimé précédemment, nous supposons que Facebook n'a pas pour intention de revendre les données brutes dont il dispose, et que la firme a plus d'intérêt à les conserver précieusement. Cambridge Analytica, entreprise travaillant avec Facebook, a donc en quelque sorte « *violé ses règles pour s'approprier des données* »[373]. Il s'agit de l'une des failles les plus impressionnantes jamais observées chez un des géants d'internet[374], mais cela signifie surtout que les mesures prises par Facebook pour protéger ces données n'était pas suffisante.

La FTC (Federal Trade Commission), autorité chargée de la protection des consommateurs américains[375] a « *décidé d'infliger une amende record de 5 milliards de dollars (environ 4,4 milliards d'euros) à Facebook* »[376] suite à l'affaire Cambridge Analytica. Du jamais vu en matière de protection des données. Cependant cette amende concerne l'ensemble des « *manquements à la protection des données personnelles des utilisateurs du réseau social* »[377]. L'incident de l'affaire Cambridge Analytica n'a fait que marquer le début des ennuis de Facebook.

---

[368] Site officiel de la CNIL, *Affaire Cambridge Analytica / Facebook*, (en ligne), *op. cit.*
[369] C. CADWALLADR et E. GRAHAM-HARRISON, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, (en ligne), *op. cit.*
[370] Site officiel de la CNIL, *Affaire Cambridge Analytica / Facebook*, (en ligne), *op. cit.*
[371] C. DE TERWANGNE, « Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel », *op. cit.*, p.343
[372] RGPD, cons. 60.
[373] C. FRATI, *Le RGPD a une génération de retard,* interview de Cyril PIERRE-BEAUSSE (en ligne), *op. cit*.
[374] C. CADWALLADR et E. GRAHAM-HARRISON, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, (en ligne), *op. cit.*
[375] A. BOERO, *Facebook : vers une amende de 5 milliards de dollars infligée aux USA*, Clubic, le 15 juillet 2019 (article en ligne disponible sur https://www.clubic.com/Internet/facebook/actualite-863927-facebook-amende-5-dollars-infligee-usa.html, dernière consultation le 06 août 2019).
[376] *Ibid.*
[377] *Ibid.*

Chapitre 3 : Les exigences du RGPD

Les différents problèmes en matière de protection des données soulevés au cours de l'examen que nous venons de faire du processus qu'est le profilage publicitaire impliquent que certaines règles doivent être respectées. Comme nous l'avons vu, le profilage n'est pas interdit, mais le RGPD vise à réguler cette activité à chacune de ses étapes[378]. La plupart des principes établis par le règlement sont directement issus de la directive 95/46/CE avant lui et certains se sont vu apporter quelques précisions. Même s'il ne permet pas de tout résoudre, son aspect coercitif au travers du montant des nouveaux plafonds de sanctions qui lui sont applicables a tendance à alerter plus sérieusement les responsables de traitement.

Nous parlerons ici en terme de devoirs et non de droits, puisque l'objectif de cette étude n'est pas d'analyser les possibilités offertes aux individus pour protéger leurs données personnelles, mais de déterminer les mesures qui devraient être prises par Facebook afin que ses activités soient conformes à RGPD. Toutefois, il est important de se rappeler que chaque prérogative dont un individu peut se prévaloir sur base du règlement, a pour corollaire une obligation dans le chef du responsable de traitement[379]. Nous évoquerons donc aussi certains droits obligeant Facebook à prendre des dispositions.

Nous analyserons le sujet en trois étapes distinctes. Nous aborderons l'article 6 du R.G.P.D avant son article 5, puisque nous estimons que dans l'ordre logique des choses il est opportun de se demander à quelles conditions un traitement peut légalement être réalisé avant de s'interroger sur la marche à suivre pour réaliser ce traitement. Nous nous attarderons ensuite sur les obligations plus spécifiques auxquelles le responsable de traitement est astreint.

Section 1 : Les conditions de licéité du traitement

Le RGPD établit six conditions qui peuvent justifier la licéité d'un traitement de donnée en son article 6. L'une d'elle au moins doit être rencontrée pour que le traitement soit considéré comme

---

[378] F. COTON et P. LIMBREE, « 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) », *op. cit.*, p. 24.
[379] N. BINCTIN, « Partie 2 : Créer une patrimonialité des données à droit constant », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles* (en ligne)*, op. cit.*, pp. 77-78

licite[380]. Nous nous concentrerons sur les deux principales d'entre elles[381], qui sont susceptibles d'être utilisées comme fondement juridique du traitement des données personnelles par Facebook à des fins de profilage publicitaire : le consentement et l'intérêt légitime.

§1. Le consentement

Le traitement sera considéré comme licite si « *la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques* »[382]. Le RGPD place cette condition en premier, appuyant ainsi le choix de la Charte Européenne des Droits Fondamentaux[383] d'en faire « *la première source de licéité des traitements de données à caractère personnel* »[384], sans pour autant instaurer de hiérarchie[385]. Le règlement a renforcé les exigences relatives à ce consentement[386]. Il doit tout d'abord être exprimé explicitement[387]. Dans le cas de Facebook, le consentement pourrait être exprimé « *en cochant une case* »[388] ou « *en optant pour certains paramètres techniques* »[389], tant que la démarche de l'utilisateur a lieu de manière « *libre, spécifique, éclairée et univoque* »[390].

A. Les caractéristiques d'un consentement valide

Le consentement n'est "libre" que si les individus disposent d'une « *véritable liberté de choix* »[391], ce qui implique entre autres que l'exécution d'un contrat ne peut dépendre du consentement à l'utilisation de données personnelles si celle-ci n'est pas absolument nécessaire[392]. Le Groupe de Travail de l'Article 29 parle d'un « *déséquilibre des rapports de force* »[393], qu'il est nécessaire de temporiser afin que les individus restent en mesure de faire leur choix librement. Cela signifie que

---

380 RGPD, art 6, §1.
381 *Ibid.*, cons. 40.
382 *Ibid.*, art 6, §1.
383 Charte des Droits Fondamentaux de l'Union Européenne, *J.O.U.E.*, C 326, du 26 octobre 2012, p. 391, art 8.
384 Y. POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.*, p. 3.
385 J.-F. PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *op. cit.*, p. 47.
386 Lignes directrices du Groupe de Travail de l'Article 29 sur le consentement au sens du règlement 2016/679, WP 259 rév.01, adoptées le 28 novembre 2017 et révisées le 10 avril 2018, (17/FR), p.16.
387 RGPD, art. 4, §11.
388 *Ibid.*, cons. 32.
389 *Ibid.*
390 *Ibid.*, art. 4, §11.
391 *Ibid.*, art. 7, §4.
392 Y. POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.*, p. 7.
393 Lignes directrices du Groupe de Travail de l'Article 29 sur le consentement au sens du règlement 2016/679, WP 259 rév.01, adoptées le 28 novembre 2017 et révisées le 10 avril 2018, (17/FR), p.6.

Facebook ne peut empêcher les internautes de s'inscrire à sa plateforme sous prétexte qu'ils refuseraient de voir leurs données exploitées à des fins de profilage publicitaire.

Le consentement doit être "spécifique" à chaque finalité rencontrée par le traitement de ses données. Si plusieurs finalités sont poursuivies, un consentement différent doit être demandé pour chacune d'entre elles[394]. De plus, chaque demande concernant un consentement doit être « *présentée sous une forme qui la distingue clairement* »[395] d'autres questions. Cette condition implique aussi que si la finalité pour laquelle les données sont traitées diffère trop amplement de celle pour laquelle elles ont été collectées, il faudra demander un nouveau consentement aux personnes concernées[396].

Le fait qu'un consentement soit "éclairé" implique que les individus disposent d'« *un contenu informationnel minimal* »[397]. Ils doivent au moins pouvoir connaître « *l'identité du responsable du traitement et les finalités du traitement auquel sont destinées les données à caractère personnel* »[398]. De plus, ces informations doivent être exprimées « *sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples* »[399]. Cette exigence soulève un problème majeur en matière de consentement, qui est souvent formulé comme une critique. Si le pouvoir lié au consentement est souvent considéré comme étant « *la concrétisation de sa maîtrise sur ses données* »[400] pour un individu, force est de constater que l'exercice de ce pouvoir dans la pratique n'est pas si fréquent. Les "conditions générales d'utilisation" sont souvent si longues que « *des études empiriques ont montré que moins d'une personne sur mille* »[401] les lit réellement. Celles de PayPal par exemple « *sont plus longues que Hamlet* »[402]. De plus, les individus ne mesurent pas toujours « *les conséquences à long terme d'un acte* »[403], et acceptent simplement les conditions établies par le distributeur d'un service.

---

394 Y. POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.*, p. 7.
395 RGPD, art. 7, §2.
396 *Ibid*., art 6, §4.
397 Y. POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.*, p. 7.
398 RGPD, cons. 42.
399 *Ibid*., art 7, §2.
400 J.-F. PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *op. cit.*, p. 46.
401 D. HOEBEKE, « Avez-vous lu les conditions générales ? "If you are not paying, you are the product"», Interview de Anne-Lise SIBONY et Nikitas MICHAIL, *in Louvains mars-avril-mai 2018* (article en ligne disponible sur https://uclouvain.be/fr/decouvrir/louvains/avez-vous-lu-les-conditions-generales.html, dernière consultation le 06 août 2019).
402 G. KOENIG, « Introduction », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles* (en ligne), *op. cit.*, p. 13.
403 D. HOEBEKE, « Avez-vous lu les conditions générales ? "If you are not paying, you are the product"», Interview de Anne-Lise SIBONY et Nikitas MICHAIL (en ligne), *op. cit*.

Le consentement est univoque s'il est exprimé « *par une déclaration ou un acte positif clair* »[404]. Cela entraine comme conséquence que « *l'indication suivant laquelle la poursuite de la navigation sur un site web équivaut à une acceptation est non recevable et que la présentation d'opt-in précochés ne peut équivaloir à un consentement* »[405]. L'effet de « *nudge* »[406] implique que « *peu de personnes modifient les paramètres par défaut d'une application ou d'un site, comme une case précochée* »[407]. De ce fait un consentement obtenu de la sorte ne peut être considéré comme étant univoque.

B. La mise en œuvre de la condition de consentement

Il n'est donc pas aisé d'obtenir un consentement qui soit totalement valide, particulièrement dans le cadre d'un traitement de type Big Data[408], mais ce n'est évidemment pas impossible. Cela nécessite une meilleure organisation de la part des responsables de traitement, et surtout une attitude compatible avec la bonne foi.

Étant donné que le règlement tend à « *faciliter l'exercice par la personne concernée des droits* »[409] qu'il lui confère, il est indiqué non seulement de formuler les demandes relatives au consentement de manière à rencontrer les exigences détaillées ci-avant, mais aussi d'aller droit au but afin que ces demandes soient abordables, puisqu'on ne peut pas « *attendre du citoyen qu'il comprenne tout* »[410]. Il est également conseillé de centraliser les demandes puisque le RGPD requiert de ne pas « *inutilement perturber l'utilisation du service* »[411] pour lequel le consentement est demandé, afin de ne pas inciter les individus à ignorer par agacement ou par découragement l'importance de la protection de leurs données personnelles[412].

---

404 RGPD, art. 4, §11.
405 Y. POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.*, pp. 8-9.
406 *Ibid*., p. 73
407 *Ibid*.
408 F. COTON et P. LIMBREE, « 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) », *op. cit.*, p. 37.
409 RGPD, cons. 50.
410 D. HOEBEKE, « Avez-vous lu les conditions générales ? "Protéger les données... by design"», Interview de Olivier PEREIRA, *in Louvains mars-avril-mai 2018* (article en ligne disponible sur https://uclouvain.be/fr/decouvrir/louvains/avez-vous-lu-les-conditions-generales.html, dernière consultation le 06 août 2019).
411 RGPD, cons. 32.
412 F. COTON et P. LIMBREE, « 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) », *op. cit.*, p. 37.

La charge de la preuve du consentement repose sur le responsable de traitement[413]. C'est pourquoi il est recommandé de désigner un « *délégué à la protection des données* »[414], qui est considéré comme étant le « *garant de l'exploitation catégorielle consentie des données du cyber-citoyen* »[415]. Il a pour mission de déterminer « *le contenu de la donnée exploitable* »[416].

Attention néanmoins au fait qu'une fois que le consentement est octroyé de manière valable, cela ne signifie pas qu'il l'est indéfiniment. Il peut effectivement être retiré à tout moment[417]. Le retrait ne remet pas en cause « *la licéité du traitement fondé sur le consentement effectué avant ce retrait* »[418], mais sa nature peut rencontrer l'une des conditions nécessaires à une demande d'effacement des données par la personne concernée[419].

§2. L'intérêt légitime

Le traitement sera également licite s'il s'avère être « *nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant* »[420].

Bien que le consentement soit placé en premier dans la liste des fondements envisageables et que l'intérêt légitime se trouve en dernière place, cela ne signifie pas pour autant que le consentement ait plus de valeur[421], puisque comme nous l'avons mentionné, il n'y a pas de hiérarchie juridique établie dans cet article[422]. Un intérêt légitime permet donc au responsable de traitement de « *traiter les données d'autrui sans son accord* »[423].

---

413 Y. POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.*, p. 9.
414 RGPD, art. 37.
415 N. BINCTIN, « Partie 2 : Créer une patrimonialité des données à droit constant », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles* (en ligne)*, op. cit.*, pp. 81-82.
416 *Ibid*., p. 88
417 RGPD, art. 7, §3.
418 *Ibid*.
419 RGPD, art. 17.
420 *Ibid*., art. 6, §1, f)
421 J.-F. PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *op. cit.*, p. 47.
422 *Ibid*.
423 *Ibid*.

A. Les conditions d'existence de l'intérêt légitime

L'intérêt doit avant toute autre chose être légitime, bien évidemment. Cela relève d'une analyse au cas par cas, étant entendu que la légitimité inclut la notion de licéité mais ne se limite pas à celle-ci[424]. Toutefois cette condition peut être remplie « *dès lors que le responsable du traitement est en mesure de poursuivre cet intérêt dans le respect de la législation sur la protection des données et d'autres législations* »[425], c'est-à-dire en rencontrant entre autres tous les principes établis par l'article 5 du RGPD, que nous développerons dans la prochaine section.

De plus le traitement en jeu doit être nécessaire à la réalisation de cet intérêt, ce qui n'implique pas qu'il doive être « *"indispensable"* »[426] mais bien qu'il ne puisse pas simplement être « *"admissible", "normal", "utile", "raisonnable" ou "opportun"* »[427].

Un intérêt légitime, doit essentiellement être « *réel et présent* »[428]. Il ne peut donc s'agir d'un intérêt théorique, potentiel, voire même purement abstrait[429]. Toutefois cet intérêt peut être de nature patrimoniale ou non sans que cela pèse dans la balance[430].

L'intérêt considéré comme légitime doit être communiqué à la personne concernée par les données susceptibles d'être traitées dans le cadre de la réalisation de cet intérêt, et ce « *d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples* »[431], afin que cette personne soit en mesure d'en comprendre l'enjeu[432].

Il faut enfin que l'intérêt légitime soit « *mis en balance* »[433] avec ceux de la personne concernée, ainsi qu'avec ses droits et libertés fondamentaux[434]. Cette évaluation se fait également «

---

424 J.-F. PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *op. cit.*, p. 52.
425 F. COTON et P. LIMBREE, « 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) », *op. cit.*, p. 34.
426 Cour eur. D.H., arrêt Silver et autres c. RU du 25 mars 1983, Publ. Cour eur. D.H. 1983, série A, n° 61, pt. 97, sur le concept de « Nécessaire dans une société démocratique ».
427 *Ibid.*
428 Avis n° 06/2014 du Groupe de Travail de l'Article 29 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 », WP 217, 9 avril 2014 (844/14/FR), p. 27
429 J.-F. PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *op. cit.*, p. 51.
430 *Ibid.*
431 RGPD, art. 12, §1.
432 J.-F. PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *op. cit.*, p. 56.
433 *Ibid.*, p. 57.
434 RGPD, art. 6, §1, f).

au cas par cas, en tenant compte de toutes les circonstances, factuelles et juridiques, de la cause »[435].

B. La tendance à préférer l'intérêt légitime comme fondement juridique

Un consentement valide étant contraignant à obtenir, il est tentant pour les responsables de traitement de se baser sur l'autre fondement légal principal qu'est l'intérêt légitime[436]. De plus l'épée de Damoclès que fait peser au-dessus de la tête du responsable de traitement le risque d'un retrait de consentement est plus inquiétante qu'une potentielle opposition[437] à un intérêt légitime. En effet, « *une telle contestation (...) sera ardue* »[438] pour les individus, ce qui assure une certaine protection aux responsables de traitement. De ce fait, au-delà du consentement, l'intérêt légitime « *est susceptible de se substituer à tous les autres fondements* »[439], ce qui est loin d'être souhaitable.

Effectivement, ce fondement « *constitue un véritable renversement de perspective* »[440] : ce ne sont plus les individus qui sont au centre de la protection au moyen de leur pouvoir de consentir ou non, mais les responsables de traitement qui peuvent se prévaloir de leurs intérêts légitimes[441]. Il est donc essentiel que les conditions de ce fondement soient appliquées avec rigueur [442], sinon quoi c'est la protection des données même qui en pâtirait : « *au lieu de renforcer l'autonomie du sujet, on aboutirait à la perpétuation de l'hétéronomie par une autre voie* »[443].

En ce qui concerne le profilage publicitaire, il peut être fondé sur l'intérêt légitime[444]. Cependant, il existe un « *droit d'opposition absolu* »[445] à cet égard pour les personnes concernées[446], c'est à dire sans que des conditions particulières soient nécessaires pour s'en prévaloir. Cependant, dans le cadre d'un traitement à des fins de profilage publicitaire impliquant

---

435 J.-F. PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *op. cit.*, p. 59.
436 F. COTON et P. LIMBREE, « 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) », *op. cit.*, p. 37.
437 RGPD, art. 21, §1.
438 J.-F. PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *op. cit.*, p. 73.
439 *Ibid.*, p. 74.
440 *Ibid.*, p. 47.
441 *Ibid.*, p. 47.
442 *Ibid.*, p. 74.
443 *Ibid.*, p. 47.
444 RGPD, cons. 47.
445 J.-F. PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *op. cit.*, p. 66.
446 RGPD, art. 21, §2 et cons. 70.

des données sensibles relevant de la vie privée des individus, seul le consentement est susceptible de servir de fondement juridique, puisque l'intérêt légitime du responsable de traitement ne suffit pas[447]. Facebook, au travers de son utilisation d'une stratégie Big Data, est susceptible de disposer de ce genre de données, que ce soit par collecte ou par déduction, et donc de les utiliser. De ce fait, il ne serait pas judicieux pour cette entreprise de se baser sur l'intérêt légitime pour justifier ses traitements à des fins de profilage publicitaire[448].

Section 2 : Les principes relatifs au traitement des données personnelles

Le fait de pouvoir justifier un traitement de données sur base d'un des fondement légitime de l'article 6 n'exempte pas le responsable de traitement de respecter certains principes dans le cadre de ce traitement[449]. Ceux énoncés à l'article 5 ont pour objectif d'« *éviter les abus* »[450].

§1. Les principes de licéité, de loyauté et de transparence des traitements

Le traitement de données personnelles doit tout d'abord être licite et avoir lieu en toute transparence vis à vis des personnes concernés par ces données[451]. Cela signifie qu'ils doivent être en mesure d'accéder aux renseignements concernant le traitement et la manière dont il sera effectué[452], mais aussi que celui-ci doit suivre les finalités annoncées dans le respect du principe de loyauté. De plus, les individus doivent être informés des « *risques, règles, garanties et droits liés au traitement* »[453] ainsi que des modalités d'exercice de ces droits[454]. De plus le RGPD établit deux listes d'informations spécifiques à fournir aux personnes concernées selon que leurs données aient été collectées directement auprès d'elles[455] ou non[456]. Cet ensemble de principes a pour objectif d'éviter que les individus soient pris par surprise ou qu'ils soient trompés d'une quelconque

---

447 RGPD, art. 9.
448 Lignes directrice du Groupe de Travail de l'Article 29 relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016.679, WP 251 rev.01, adoptées le 3 octobre 2017 et révisées le 6 février 2018, (17/FR), p.16.
449 Y. POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.*, p. 18.
450 J.-F. PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *op. cit.*, p. 43.
451 RGPD, art. 5, §1, a).
452 *Ibid.*, art. 12 et cons. 39.
453 *Ibid.*, cons. 39.
454 *Ibid.*, art. 12.
455 *Ibid.*, art. 13.
456 *Ibid.*, art. 14.

manière[457] sur le traitement auquel ils consentent ou sur celui qui leur est imposé par un intérêt légitime.

Comme nous l'avons expliqué, dans le cadre de l'affaire Cambridge Analytica, c'est entre autres d'un problème de loyauté envers les personnes concernées qu'il s'agissait[458] et par extension d'un problème de transparence[459]. En effet il avait été annoncé que les données récoltées serviraient à alimenter une étude académique or celles-ci ont en réalité été exploitées à des fins de prospection commerciale et politique[460].

Facebook a récemment amélioré une de ses fonctionnalités, qui permet désormais à ses utilisateurs de mieux comprendre l'utilisation qui est faite de leurs données à des fins publicitaires, mais aussi de contrôler les publicités qui leur sont proposées[461]. Reste à voir si cette démarche est mise en œuvre de manière suffisamment honnête que pour rencontrer le principe de transparence.

§2. Le principe de limitation des finalités

Les finalités du traitement doivent être « *déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités* »[462]. Le traitement des données doit donc avoir des « *buts spécifiques* »[463]. Ceux-ci doivent être déterminés en amont du traitement, afin de les soumettre au consentement des utilisateurs ou de justifier un intérêt légitime[464]. Si les finalités pour lesquelles des données sont traitées changent, il faut vérifier si elles sont compatibles avec les finalités annoncées, ou bien demander un nouveau consentement s'il n'est pas question d'un autre fondement établi par l'article 6[465].

---

[457] C. DE TERWANGNE, « Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel », *op. cit.*, p. 342.
[458] Ibid., p. 343.
[459] RGPD, cons. 60.
[460] C. DE TERWANGNE, « Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel », *op. cit.*, p. 343.
[461] M. SZADKOWSKI, *Facebook donne un peu plus de détails sur le ciblage publicitaire de ses utilisateurs*, Le Monde, le 12 juillet 2019 (article en ligne disponible sur https://www.lemonde.fr/pixels/article/2019/07/12/facebook-donne-un-peu-plus-de-detail-sur-le-ciblage-publicitaire-de-ses-utilisateurs_5488626_4408996.html?utm_medium=Social&utm_source=Facebook&fbclid=IwAR3WAtN26v5iXjasaiI1yWvARUhW5qoC35Z44O25IMbkHoC6E1L4kMPgNzE#Echobox=1562947577, dernière consultation le 06 août 2019).
[462] RGPD, art. 5, §1, b).
[463] A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, pp. 20-21.
[464] F. COTON et P. LIMBREE, « 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) », *op. cit.*, p. 31.
[465] RGPD, art. 6, §4.

Ce principe a des conséquences sur la notion même de Big Data, qui comme nous l'avons vu a pour optique de collecter un maximum de données et d'observer quels résultats en tirer[466] et n'implique donc pas de fixer des finalités au préalable. En vue de respecter le règlement, il serait bon d'adopter une méthode permettant de déterminer les finalités du traitement.

§3. Le principe de minimisation des données

Les données utilisées dans le cadre d'un traitement doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* »[467]. Cela signifie que le responsable de traitement ne peut donc traiter que les données nécessaires à l'accomplissement des finalités qu'il a déterminées, ce qui concerne tant leur quantité que leur qualité[468]. Il devra aussi préférer l'utilisation de données anonymisées, pseudonymisées et non-sensibles à celle de données intrusives[469]. Ce principe implique également que le traitement de données personnelles ne peut avoir lieu si d'autres moyens permettent de manière raisonnable d'atteindre ces finalités[470].

L'utilisation des techniques liées au Big Data va également à l'encontre de ce principe. L'analyse de données en Big Data se base actuellement sur une quantité indéterminée de ces données, que les responsables veulent le plus nombreuses possibles afin d'alimenter leurs algorithmes pour produire un maximum d'informations[471]. Une solution à cette opposition entre le principe de minimisation des données (ainsi que celui de limitation des finalités) et le Big Data est envisageable au travers du concept de *Smart Data*. Il s'agit d'une « *nouvelle approche du traitement des données, consistant à extraire de l'immense masse de données procurée par le big data les informations les plus pertinentes pour mener des campagnes marketing* »[472]. Cela implique de préférer la qualité des données à leur quantité[473] et d'évaluer quelles sont celles qui sont «

---

466 F. COTON et P. LIMBREE, « 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) », *op. cit.*, p. 30.
467 RGPD, art. 5, §1, c).
468 A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, p. 23.
469 *Ibid.*, p. 24.
470 RGPD, cons. 39.
471 A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, p. 23.
472 Smart Data, E-marketing Glossaire (article en ligne disponible sur https://www.e-marketing.fr/definitions-glossaire/smart-data-254969.htm, dernière consultation le 06 août 2019).
473 *Adieu Big Data, bonjour Smart Data !*, E-marketing, le 29 juin 2018 (article en ligne disponible sur https://www.e-marketing.fr/Thematique/data-1091/breve/adieu-big-data-bonjour-smart-data-332456.htm, dernière consultation le 06 août 2019).

nécessaires, simplement utiles, ou d'un intérêt minime »[474]. Cette technique de sélection se base sur l'utilisation de « *logiciels dédiés* »[475] par des professionnels. Le *Smart Data* permet à la fois d'améliorer la stratégie commerciale du profilage publicitaire et de se rapprocher des exigences du RGPD[476].

§4. Le principe d'exactitude des données

Le responsable de traitement ne peut traiter que des données personnelles « *exactes et, si nécessaire, tenues à jour* »[477]. Les données « *objectivement inexactes* »[478] – on ne parle donc pas de jugements de valeur ou d'avis subjectifs[479] – doivent être dans la mesure du possible « *effacées ou rectifiées sans tarder* »[480]. Ce principe relève d'une « *obligation de moyen* »[481] et non de résultat. Toutefois les personnes concernées peuvent elles-mêmes demander une rectification de leurs données personnelles.[482]

Par ailleurs, bien que le principe de minimisation des données implique que la quantité de données ne puisse être excessive, elle doit être suffisante afin d'éviter que les algorithmes ne produisent des données erronées[483].

§5. Le principe de limitation de la conservation

Les données personnelles ne peuvent être conservées au-delà de la durée « *nécessaire au regard des finalités pour lesquelles elles sont traitées* »[484]. Cette durée doit être limitée au « *strict minimum* »[485]. Le responsable de traitement devrait fixer ces délais à l'avance pour garantir le respect de ce principe[486]. Une fois la finalité atteinte ou le délai fixé dépassé, les données devront être effacées

---

474 A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, p. 24.
475 Smart Data, E-marketing Glossaire (en ligne), *op. cit*.
476 *Adieu Big Data, bonjour Smart Data !*, E-marketing, le 29 juin 2018 (en ligne), *op. cit*.
477 RGPD, art. 5, §1, d).
478 A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, p. 25.
479 *Ibid.*
480 RGPD, art. 5, §1, d).
481 A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, p. 25.
482 RGPD, art. 16.
483 A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, p. 24.
484 RGPD, art. 5, §1, e).
485 *Ibid.*, cons. 39.
486 *Ibid.*

mais pourront aussi être anonymisées[487] dans la mesure où le risque de réidentification serait inexistant.

Dans le cadre du Big Data, le responsable du traitement est pourtant tenté de « *conserver les données pour pouvoir éventuellement les réutiliser plus tard* »[488], mais cela va à l'encontre de ce principe.

§6. Les principes d'intégrité et de confidentialité

Le traitement de données personnelles doit mettre en œuvre les « *mesures techniques ou organisationnelles* »[489] destinées à « *garantir une sécurité appropriée* »[490] ainsi que la confidentialité[491] des données. Ces mesures doivent pouvoir empêcher « *l'accès non autorisé à ces données et à l'équipement utilisé pour leur traitement* »[492] de même que « *le traitement non autorisé ou illicite* »[493] et « *la perte, la destruction ou les dégâts d'origine accidentelle* »[494] de ces données. Le RGPD tend à renforcer ce principe[495] afin de mettre en place un « *niveau de sécurité adapté au risque* »[496], tant pour les individus que pour les responsables de traitement[497]

Ces "mesures" peuvent entre autres consister en « *la pseudonymisation et le chiffrement des données à caractère personnel* »[498], « *des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement* »[499] ou « *de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique* »[500], ou encore « *une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement* »[501].

---

[487] A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, p. 24.
[488] *Ibid.*, p. 23.
[489] RGPD, art. 5, §1, f).
[490] *Ibid.*
[491] RGPD, cons. 39.
[492] *Ibid.*
[493] RGPD, art. 5, §1, f).
[494] *Ibid.*
[495] RGPD, cons. 7.
[496] *Ibid.*, art. 32, §1.
[497] N. BINCTIN, « Partie 2 : Créer une patrimonialité des données à droit constant », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles* (en ligne)*, op. cit.*, p. 77.
[498] RGPD, art. 32, §1, a).
[499] *Ibid.*, art. 32, §1, b).
[500] *Ibid.*, art. 32, §1, c).
[501] *Ibid.*, art. 32, §1, d).

Si malgré ces précautions (ou à défaut de ces précautions) il devait advenir que la protection des données personnelles ait échoué, qu'une violation soit advenue, et que celle-ci soit de nature à « *engendrer un risque pour les droits et libertés des personnes physiques* »[502], l'APD compétente et les personnes concernées devront être prévenues au plus vite[503]. Dans le cas de Cambridge Analytica, il a fallu presque trois ans pour que le scandale éclate : Facebook avait repéré la faille depuis 2015, et ce n'est qu'en 2018 que la nouvelle a éclaté au grand jour[504].

Section 3 : Les obligations du responsable de traitement

Le RGPD établit parmi les « *obligations générales* »[505] du responsable de traitement deux exigences majeures et pertinentes dans le cadre de notre analyse, que nous allons développer dans cette section. Celle que nous aborderons en premier impose au responsable de traitement une manière particulière de mettre en œuvre les règles relatives à la protection des données personnelles : elle se retrouve dans deux notions exprimées en anglais par le terme de *Privacy*, à savoir le *Privacy by design* et le *Privacy by default*. La seconde exigence que nous expliquerons est celle d'*accountability*, qui impose désormais aux responsables de traitement de pouvoir démontrer qu'ils ont correctement mis leur traitement en conformité au RGPD

§1. Les notions de Privacy

Il revient au responsable de traitement d'intégrer les deux notions de *Privacy* dans sa « *politique de mise en conformité* »[506]. Celles-ci impliquent d'une part de prendre en considération la « *protection des données dès la conception* »[507] du traitement plutôt qu'*a posteriori* [508], mais aussi d'organiser leurs paramètres de confidentialité de telle sorte que les individus disposent d'une «

---

[502] RGPD, art. 33, §1.
[503] *Ibid.*, art. 33, §1 et 34, §1
[504] C. CADWALLADR et E. GRAHAM-HARRISON, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, (en ligne), *op. cit.*
[505] RGPD, art. 24-31.
[506] A. DELFORGE, « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.*, p. 371.
[507] RGPD, art. 25.
[508] A. DELFORGE, « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.*, p. 387.

protection des données par défaut »[509]. Cela passe par un changement radical de point de vue depuis la création des systèmes de traitement jusqu'à la mise à disposition du service aux individus[510].

A. La protection des données dès la conception (*privacy by design*)

L'exigence de protection des données dès la conception nécessite la mise en œuvre « *des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données* »[511] que nous avons détaillés dans la section précédente. Cette démarche déplace la charge de la protection des données personnelles des individus vers le responsable de traitement[512].

Les mesures évoquées peuvent consister en une mise à jour en profondeur des logiciels de traitement, ou même par le remplacement de ceux-ci, mais ce n'est pas obligatoire s'il est possible de garantir la protection des données personnelles par des moyens moins radicaux[513]. Il reste que la conception de « *logiciels "user-friendly"* »[514] est la méthode idéale, qui permet à la fois d'aider les individus à mieux maitriser leurs données personnelles et d'assurer une meilleure transparence de la part du responsable de traitement[515].

B. La protection des données par défaut (*privacy by default*)

L'exigence de protection des données par défaut implique l'implémentation de « *mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées* »[516], ce qui concerne à la fois l'étendue de la collecte, celle du traitement, la durée de la rétention et l'accessibilité à des tiers[517].

---

[509] RGPD, art. 25.
[510] *Ibid.*, cons. 78.
[511] *Ibid.*, art. 25, §1.
[512] A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, pp. 306-307.
[513] A. DELFORGE, « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.*, p. 390.
[514] *Ibid.*, p. 388
[515] *Ibid.*
[516] RGPD, art. 25, §2
[517] *Ibid.*

Dans la pratique, sur Facebook, cela correspond à la configuration par défaut des profils d'utilisateurs en mode privé lors de leur inscription[518]. En d'autres mots, ces profils doivent être « *par défaut conformes aux principes généraux de la protection des données* »[519]. Ce n'est que par la suite que les utilisateurs doivent pouvoir déterminer par eux-mêmes s'ils souhaitent modifier leurs paramètres de confidentialité[520]. Par extension, cela signifie que Facebook doit configurer ces paramètres par défaut de telle sorte qu'ils ne permettent pas le profilage, et que le consentement des utilisateurs doit être demandé avant de commencer à les "profiler"[521]. Ce consentement ne pourrait être octroyé par défaut, via des cases pré-cochées ou une abstention[522].

Une configuration inverse pose problème dans la mesure où les individus ne font que rarement la démarche de chercher comment modifier ces paramètres et de le faire[523]. Facebook, qui se base sur cette configuration inverse, a « *continuellement accru la visibilité des données disponibles dans son mode par défaut* »[524]. C'est une des modifications principales que le réseau social devrait apporter à ses pratiques.

§2. Le concept d'"accountability"

Le responsable de traitement doit « *s'assurer* »[525] de sa mise en conformité au règlement, en particulier en ce qui concerne les risques en matière de sécurité des données personnelles[526]. Pour ce faire, une « *analyse minimale* »[527] des mesures qu'il prend à cette fin est nécessaire. Celle-ci est à ne pas confondre avec l'« *analyse d'impact relative à la protection des donnés* »[528] prévue par le

---

518 A. DELFORGE, « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.*, p. 391.
519 A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, pp. 306-307.
520 A. DELFORGE, « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.*, p. 391.
521 A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, pp. 306-307.
522 RGPD, cons. 32.
523 A. DELFORGE, « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.*, p. 391.
524 I. LANDREAU, L. LÉGER et V. PEZ-PÉRARD, « Partie 1 : Les aspects socio-économiques et éthiques des données personnelles », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles* (en ligne), *op. cit.*, p. 40.
525 RGPD, art. 24, §1.
526 N. BINCTIN, « Partie 2 : Créer une patrimonialité des données à droit constant », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles* (en ligne), *op. cit.*, pp. 77-78.
527 A. DELFORGE, « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.*, p. 384.
528 RGPD, art. 35.

R.G.P.D, qui est d'une envergure plus conséquente et n'est pas obligatoire pour tous les types de traitement[529].

Le concept d'*accountability* implique que le responsable du traitement doit également pouvoir « *démontrer* »[530] qu'il respecte les principes relatifs au traitement des données personnelles[531], qu'il a mis en œuvre les principes relatifs à la notion de Privacy[532] expliqués ci-dessus et que ses pratiques en général sont conformes au R.G.P.D[533]. Toutefois, il ne peut se contenter de prendre des mesures en vue d'assurer la protection des données personnelles : il doit également veiller à ce que ces mesures soient effectives et efficaces[534].

Si le terme même d'*accountability,* emprunté à l'anglais, n'apparaît nulle part dans le RGPD, le concept transparaît dans cette obligation qu'il impose au responsable de traitement[535]. La directive avant lui évoquait implicitement ce mécanisme[536], mais sa mise en place par le règlement établit un « *changement de paradigme* »[537] majeur.

Cette obligation relève en réalité d'un mécanisme de reddition de comptes[538], qui consiste à « *laisser plus de marge de manœuvre aux responsables de traitement et à leur(s) sous-traitant(s) pour assurer la conformité de leurs traitements* »[539], autrement dit à les « *responsabiliser* »[540], en leur imposant en contrepartie d'être prêt à prouver cette conformité en cas de contrôle[541]. Il y a deux raisons à ce changement d'approche : d'une part, les contrôles préalables à la mise en place d'un système de traitement étaient très contraignants à effectuer pour les APD[542], et d'autre part les sanctions désormais applicables aux violations des principes établis par le RGPD sont supposées

---

529 A. DELFORGE, « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.*, p. 384.
530 RGPD, art. 24, §1.
531 *Ibid.*, art. 5, §2.
532 A. DELFORGE, « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.*, p. 384.
533 RGPD, art. 24, §1.
534 B. DOCQUIR, « Chapitre 4. - Principes généraux de la protection des données », *in Droit du numérique*, Bruxelles, Larcier, 2018, p. 416.
535 A. DELFORGE, « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.*, p. 383.
536 *Ibid.*, p. 382
537 N. BINCTIN, « Partie 2 : Créer une patrimonialité des données à droit constant », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles* (en ligne)*, op. cit.*, pp. 77-78.
538 A. DELFORGE, « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.*, p. 382.
539 *Ibid.*, p. 371.
540 *Ibid.*, p. 382
541 *Ibid.*, p. 371.
542 *Ibid.*, p. 382

être une motivation suffisante pour le responsable de traitement de respecter le règlement[543]. Cela marque le passage de la protection des données personnelles à « *l'ère de la compliance* »[544].

[543] D. HOEBEKE, « Avez-vous lu les conditions générales ? "Protéger les données... by design"», Interview de Olivier PEREIRA (en ligne), *op. cit*.

[544] N. BINCTIN, « Partie 2 : Créer une patrimonialité des données à droit constant », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles* (en ligne)*, op. cit.*, pp. 77-78.

Chapitre 4 : Approche critique sur la pertinence du RGPD

Des développements des chapitres précédents découlent plusieurs observations et impliquent surtout quelques questionnements dont nous ouvrirons les portes dans ces quelques lignes clôturant notre étude.

Section 1 : Les possibilités d'extension de la philosophie du RGPD

§1. La valeur d'exemple

L'une des questions que nous nous posons est l'éventualité d'une étendue de l'esprit du RGPD au reste du monde. Il est envisageable que la démarche entreprise par l'Europe soit suivie ailleurs et que les avantages que nous reconnaissons à ce règlement puissent inspirer d'autres législateurs. En effet, le cadre normatif imposé par le règlement que nous avons détaillé dans le troisième chapitre représente un canevas et une philosophie qui pourrait intéresser d'autres pays.

§2. Le point de vue des États-Unis

Cependant, comme nous l'avons évoqué dans le cadre du premier chapitre, l'étendue du champ d'application du RGPD est plutôt de nature à contrarier les pays qui se sentent envahis par la législation européenne[545], et nous supposons que cela concerne en particulier les États-Unis puisque pour le moment ce sont majoritairement des grandes entreprises américaines qui sont visées par les sanctions relatives au règlement. Le territoire américain accueille effectivement de nombreuses entreprises similaires à Facebook[546] dont le modèle économique est également basé sur la monétisation des données, et qui posent dès lors le même genre de problème.

C'est pourquoi il ne faut pas être trop optimiste à cet égard en ce qui concerne les États-Unis, qui représentent pourtant un élément clé en matière de protection des données. Ce pays n'aurait que peu d'intérêts à « *censurer ce que font les grandes entreprises qui sont leur fleuron mondial et qui sont en position de monopole dans leurs activités respectives* »[547]. L'amende magistrale imposée à

[545] N. MICHAIL, « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *op. cit.*, p. 71.
[546] J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, p. 236.
[547] C. FRATI, *Le RGPD a une génération de retard,* interview de Cyril PIERRE-BEAUSSE (en ligne), *op. cit*.

Facebook par la FTC suite à l'affaire Cambridge Analytica pourrait n'être qu'une manière de sauver les apparences et de feindre une coopération avec l'Europe en ce qui concerne la protection des données personnelles. Effectivement l'impact de cette amende a finalement été relativement minime pour les finances de cette entreprise[548].

Section 2 : L'efficacité de l'application du RGPD

§1. Les défauts et lacunes du RGPD

Malgré la panoplie de bonnes intentions dont s'est armé le législateur, nous nous demandons si le RGPD n'a pas une « *génération de retard* »[549]. La manipulation opérée sur les individus au travers de l'utilisation de leurs données personnelles va aujourd'hui bien plus loin que le simple profilage publicitaire : comme nous l'avons observé, dans le cadre de l'affaire Cambridge Analytica, c'est d'une manipulation politique qu'il était question[550]. Les dérives pourraient prendre encore plus d'ampleur dans les mois et les années à venir. Il est dès lors pertinent de se demander si le cadre de protection établi par le RGPD est suffisant pour faire face à ce genre de complications, en particulier au vu de la potentielle indifférence des grandes entreprises que nous venons d'évoquer[551].

De plus, certains estiment que le règlement entraîne une « *approche administrative* »[552], voire même « *une vision bureaucratique de la vie privée* »[553], qui est trop lourde et complexe à mettre en oeuvre et qui n'assure pas la protection effective de celle-ci sur le terrain.

Il faudra attendre avant de pallier réellement les manquements du RGPD. Les réponses devront venir de la C.J.U.E, du Comité Européen de la Protection des Données (remplaçant le Groupe de Travail de l'Article 29), et de législations à venir destinées à compléter le règlement, notamment le «

---

548 A. BOERO, *Facebook : vers une amende de 5 milliards de dollars infligée aux USA*, (en ligne), *op. cit.*
549 C. FRATI, *Le RGPD a une génération de retard,* interview de Cyril PIERRE-BEAUSSE (en ligne), *op. cit*.
550 *Ibid.*
551 *Ibid.*
552 *Ibid.*
553 D. HOEBEKE, « Avez-vous lu les conditions générales ? "Un droit fondamental"», Interview de Alain STROWEL, *in Louvains mars-avril-mai 2018* (article en ligne disponible sur https://uclouvain.be/fr/decouvrir/louvains/avez-vous-lu-les-conditions-generales.html, dernière consultation le 06 août 2019).

Règlement Vie Privée et Communications Electroniques »[554] qui viendra remplacer la directive de 2002, et qui n'en est toujours qu'au stade de proposition.

§2. La position de force de Facebook

Outre les défauts du règlement soulevés précédemment, il y a lieu de s'interroger sur l'efficacité réelle du RGPD face à des entités comme Facebook. S'il ne fait aucun doute que les entreprises et organisations de petite envergure se tracassent du montant des amendes qu'il a instauré, il n'en va pas de même pour les GAFA, qui représentent pourtant un risque beaucoup plus conséquent en ce qui concerne la protection des données personnelles[555]. En effet, comme nous l'avons évoqué dans la section précédente, les moyens financiers dont les Géants du Web disposent leur permettent de ne pas se tracasser outre mesure des conséquences de leur comportement en la matière[556]. Cela leur laisse dès lors l'occasion d'amasser toujours plus de bénéfices en continuant à exploiter les données personnelles des individus[557].

Malgré sa relative indifférence à l'égard des sanctions financières, Facebook a bien un intérêt particulier à faire mine de respecter les principes relatifs à la protection des données personnelles. Cela lui permet de maintenir la confiance de ses utilisateurs[558]. En effet les récents scandales dont le réseau social a fait l'objet a créé une vague de méfiance parmi les individus, qui vont parfois même jusqu'à quitter la plateforme[559]. Comme nous l'avons vu, dans la pratique cela n'empêche pas Facebook de continuer à les tracer. Cependant l'image de la société a également une valeur. Celle-ci a donc entrepris de prendre certaines mesures[560], comme nous l'avons relevé par exemple en ce qui concerne la transparence des ciblages publicitaires, qui ont principalement pour objectif de rassurer ses utilisateurs, et de leur donner l'impression d'avoir le contrôle. La Commission Européenne et

---

554 Proposition de Règlement n° 03/2017 du Parlement Européen et du Conseil, concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»), *C.O.M.* (2017) 10 en cours.
555 C. FRATI, *Le RGPD a une génération de retard,* interview de Cyril PIERRE-BEAUSSE (en ligne), *op. cit*.
556 *Ibid.*
557 *Ibid.*
558 C. GAYREL, « Chapitre 12. - L'expansion des standards européens de protection des données dans le monde », *op. cit.*, p. 481.
559 A. PERRIN, *Americans are changing their relationship with Facebook*, Pew Research Center, le 5 septembre 2018 (article en ligne disponible sur http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/, dernière consultation le 06 août 2019).
560 A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 278.

les APD semblent satisfaites de la plupart des efforts de Facebook en matière de transparence[561]. Nous restons pour notre part sceptiques quant à l'efficacité de ces prétendues adaptations dans le cadre d'une réelle mise en conformité à RGPD.

Nous craignons que l'intention du règlement de poursuivre simultanément deux buts essentiels mais fondamentalement opposés ne soit de nature à lui porter préjudice. En effet, en voulant protéger les données personnelles tout en encourageant le flux de ces données et l'économie numérique[562], il est probable que le RGPD manque d'efficacité sur le terrain. Cependant il n'est pas possible d'aborder l'une de ces problématiques sans se préoccuper de l'autre. Ce nouveau règlement ne pouvait se permettre d'être trop vindicatif, puisque l'enjeu de la protection des données ne peut pas représenter un risque de détruire cette économie. Certes, il aurait peut-être été plus intéressant dans le cadre de la protection des données personnelles d'interdire tout bonnement le profilage publicitaire et il y a d'ailleurs lieu de se demander pourquoi cela n'a pas été fait. La réponse est simple : le profilage publicitaire représente un des nombreux rouages intégrés aux mécanismes actuels de l'économie mondiale, et une marche-arrière radicale en la matière aurait d'énormes répercussions sur celle-ci.

Section 3 : Les alternatives envisageables

Il existe des possibilités d'améliorer la protection des données des utilisateurs de Facebook qui n'ont pas encore été explorées par la législation. Il nous paraît opportun de relever certaines de ces alternatives.

§1. La possibilité de rendre le service payant

Certains proposent de rendre le service du réseau social payant[563]. Certes, cela permettrait d'ôter toute justification à l'utilisation massive des données, mais nous ne pensons pas que cela

---

[561] Communiqué de presse de la Commission Européenne, *À la demande de la Commission européenne et des autorités de protection des consommateurs, Facebook change ses conditions d'utilisation et précise l'utilisation des données fournies par les consommateurs*, le 9 avril 2019 (disponible sur http://europa.eu/rapid/press-release_IP-19-2048_fr.htm, dernière consultation le 06 août 2019).

[562] J.-F. PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *op. cit.*, p 41-42

[563] « Résumé », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles*, (Sous la direction de LÉGER L.), janvier 2018 (disponible sur https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf, dernière consultation le 06 août 2019), p. 10.

règlerait le problème pour autant. Premièrement nous estimons que cela n'empêcherait pas Facebook de continuer à monétiser les données personnelles des individus (cela permettrait seulement d'accroître ses bénéfices et de le rendre encore plus imperméable à toute amende). Deuxièmement nous ne pensons pas que la mise en œuvre de cette hypothèse soit réaliste, dans la mesure où cela irait tout à fait à l'encontre de la conception que les individus ont des réseaux sociaux.

§2. La possibilité de se faire payer par le service

Une rémunération des individus pour la récolte et l'utilisation de leurs données personnelles[564] est également envisagée par certains auteurs de doctrine, mais nous ne sommes pas certains qu'il s'agisse d'une solution viable sur le long terme. En effet, même accompagnée d'une régulation conséquente, nous pensons que cette pratique équivaudrait probablement à une perte de contrôle encore plus inquiétante des personnes sur leurs données. La plupart des individus, qui consentent déjà beaucoup trop facilement à l'utilisation de leurs données par agacement ou par inconscience, seraient d'autant plus tentés de le faire s'ils étaient rétribués pour cela.

§3. L'hypothèse d'une segmentation du service

Une solution certes moins conséquente mais plus abordable, serait l'élaboration de « *niveaux de service* »[565]. Cela permettrait aux individus d'avoir le choix entre plusieurs degrés de service, du plus basique au plus complet[566], « *auxquels est associée chaque fois la collecte de données complémentaires* »[567]. Chacun de ces niveaux de service impliquerait un consentement spécifique. Les individus qui se tracassent de la protection de leurs données personnelles pourraient tout de même accéder à une version minimaliste du réseau social. Ceux qui souhaitent disposer d'une version plus complète pourraient quant à eux consentir à une plus large intrusion dans leur vie privée. Nous trouvons cette solution réaliste et pratique dans le cas de Facebook mais également dans de nombreuses autres situations impliquant un traitement de données personnelles. Cependant, elle n'est – pour autant – pas optimale, à cause de cette tendance généralisée consistant à bien trop vite abandonner son consentement.

---

564 G. KOENIG, « Introduction », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles* (en ligne), *op. cit.*, p. 17.
565 Y. POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.*, p. 33.
566 *Ibid.*
567 *Ibid.*

Conclusion

Cette étude a été l'occasion d'éclairer divers aspects de la problématique qui nous occupe, non seulement en ce qui concerne le comportement adopté par Facebook et ses semblables en matière de protection des données personnelles, mais aussi au sujet du RGPD et de ses implications.

Tout d'abord nous nous sommes assurés au cours du premier chapitre que Facebook rentrait bien dans le champ d'application du nouveau règlement européen concernant la protection des données personnelles, et ce sous ses différents aspects : matériel, personnel et territorial. Nous avons également pu évoquer les manières de faire appliquer ce règlement dans la pratique, en particulier au travers des APD.

Les développements du deuxième chapitre illustrent le fait que le phénomène de monétisation des données au travers du profilage publicitaire incite les opérateurs tels que Facebook à élaborer des techniques toujours plus précises pour améliorer ce profilage à chacune de ses étapes. Il est regrettable que le seul paramètre qui n'ait pas été suffisamment pris en compte par les Géants du Web jusqu'à aujourd'hui soit celui de la protection de ces informations et des personnes qu'elles concernent, les données des individus étant considérées comme un simple bien monnayable et générateur de profits. Pourtant, la seule définition qu'a le RGPD du profilage met en exergue son aspect intrusif et « *permet de comprendre qu'il s'agit d'une mesure potentiellement très insidieuse, pouvant aller jusqu'à permettre la manipulation de la personne qui en fait l'objet* »[568], comme nous avons pu le constater entre autres avec l'affaire Cambridge Analytica.

Le troisième chapitre, dans le cadre duquel nous avons analysé plus précisément les règles du R.G.P.D applicables au profilage opéré par Facebook sur les internautes, a permis de mieux comprendre les intentions du législateur dans la rédaction de ce règlement. Nous y avons en réalité retracé les points essentiels d'une mise en conformité au RGPD, et les liens que nous avons faits avec les activités de Facebook ont mis en lumière les mesures qui permettraient à l'entreprise de rencontrer ces exigences.

---

[568] J.-F. PUYRAIMOND, « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *op. cit.*, p. 68.

Au cours du quatrième chapitre nous avons émis certaines observations relatives aux défauts, aux lacunes et au manque d'efficacité pratique du règlement face aux Géants d'Internet. Nous avons ouvert des pistes de réflexion au travers de différentes alternatives, qui renvoient néanmoins toutes à une même problématique : la nécessité d'une implication plus importante des individus eux-mêmes dans la protection de leurs données.

Nous conclurons donc cette étude sur une observation à la fois pessimiste et optimiste. Le problème de fond repose sur deux éléments, que la loi ne pourrait complètement compenser.

D'une part le fait que la possibilité de protéger pleinement les données personnelles repose majoritairement « *sur la bonne volonté des grands opérateurs du Net* »[569], qui disposent aujourd'hui d'un pouvoir beaucoup trop conséquent. Théoriquement, Facebook pourrait tout à fait se conformer aux exigences du RGPD, mais nous supposons qu'il a en réalité plus d'intérêts à préférer la productivité à la légalité.

D'autre part le manque de conscience et de sensibilisation de la population par rapport à l'importance de la protection de leurs données[570]. Toutefois, on observe une évolution progressive, « *les gens, petit à petit, s'accaparent leurs droits* »[571].

S'il est essentiel de prendre le problème à sa source en s'inquiétant du comportement des responsables de traitement, comme nous l'avons fait dans le cadre de cette étude, il est d'autant plus important d'inciter les individus à prendre les choses en main, à prendre le temps de s'inquiéter de la protection de leurs données personnelles et à user pleinement de l'arsenal juridique qui leur est octroyé…

---

[569] A. GROSJEAN, « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 310.
[570] B. DOUCET, « Avez-vous lu les conditions générales ? "GDPR, une occasion manquée ?"» *in Louvains mars-avril-mai 2018* (en ligne), *op. cit.*
[571] C. FRATI, *Le RGPD a une génération de retard,* interview de Cyril PIERRE-BEAUSSE (en ligne), *op. cit*.

BIBLIOGRAPHIE

Législation

- Traité sur le Fonctionnement de l'Union européenne (version consolidée), *J.O.U.E.*, C 326, du 26 octobre 2012, p. 001, art 16.

- Charte des Droits Fondamentaux de l'Union Européenne, *J.O.U.E.*, C 326, du 26 octobre 2012, p. 391, art 8.

- Directive (CE) n° 46/1995 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, p. 031, art 25.

- Directive (CE) n° 58/2002 du Parlement européen et du Conseil du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *J.O.C.E.*, L 201, du 31 juillet 2002, p. 037.

- Règlement (CE) n° 593/2008 du Parlement européen et du Conseil du 17 juin 2008, sur la loi applicable aux obligations contractuelles (Règlement Rome I), *J.O.U.E.*, L 177, du 4 juillet 2008, p. 006, art 6.

- Règlement (UE) n° 679/2016 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119, 4 mai 2016, p. 001.

- Décision d'exécution (UE) 1250/2016 de la Commission du 12 juillet 2016, conformément à la directive 95/46/CE du Parlement européen et du Conseil, relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, notifiée sous le numéro C/ 2016/4176, *J.O.U.E.*, L 207, du 1er août 2016, p. 001.

- Proposition de Règlement n° 03/2017 du Parlement Européen et du Conseil, concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»), *C.O.M.* (2017) 10 en cours.

- Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018, p. 989.

Publications officielles

- Document de travail du Groupe de Travail de l'Article 29 sur les questions de protection des données liées à la technologie RFID (radio-identification), WP 105, 19 janvier 2005 (01248/07/FR).

- Avis n° 4/2007 du Groupe de Travail de l'Article 29 sur le concept de données à caractère personnel, WP 136, 20 juin 2007 (10107/05/FR).

- Avis n° 1/2008 du Groupe de Travail de l'Article 29 sur les aspects de la protection des données liés aux moteurs de recherche, WP 148, 4 avril 2008 (00737/FR).

- Avis n° 5/2009 du Groupe de Travail de l'Article 29 sur les réseaux sociaux en ligne, WP 163, 12 juin 2009 (01189/09/FR).

- Avis n° 1/2010 du Groupe de Travail de l'Article 29 sur les notions de responsable du traitement et de sous-traitant, WP 169, 16 février 2010 (00264/10/FR).

- Avis n° 8/2010 du Groupe de Travail de l'Article 29 sur le droit applicable, WP 179, 16 décembre 2010, (0836-02/10/FR).

- Avis n° 06/2014 du Groupe de Travail de l'Article 29 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 », WP 217, 9 avril 2014 (844/14/FR).

- Update of Opinion 8/2010 of the Working Party 29 on applicable law in light of the CJEU judgment in Google Spain, WP 179 update, 16 décembre 2015 (176/16/EN).

- Avis n° 7/2015 du Contrôleur européen de la protection des données sur les défis des données massives, 19 novembre 2015.

- Lignes directrice du Groupe de Travail de l'Article 29 relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016.679, WP 251 rev.01, adoptées le 3 octobre 2017 et révisées le 6 février 2018, (17/FR).

- Lignes directrices du Groupe de Travail de l'Article 29 sur le consentement au sens du règlement 2016/679, WP 259 rév.01, adoptées le 28 novembre 2017 et révisées le 10 avril 2018, (17/FR).

Jurisprudence

Juridictions européennes

- Cour eur. D.H., arrêt Silver et autres c. RU du 25 mars 1983, Publ. Cour eur. D.H. 1983, série A, n° 61.

- Arrêt Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12, EU:C:2014:317.

- Arrêt Weltimmo s. r. o./Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, EU:C:2015:639.

- Arrêt Patrick Breyer/Bundesrepublik Deutschland, C−582/14, EU:C:2016:779.

- Arrêt Peter Nowak/Data Protection Commissioner, C-434/16, EU:C:2017:994.

- Arrêt Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein GmbH (arrêt Fanpage), C-210/16, EU:C:2018:388.

- Arrêt Tietosuojavaltuutettu, C-25/17, EU:C:2018:551.

- Arrêt Fashion ID GmbH & Co. KG/Verbraucherzentrale NRW eV, C-40/17, EU:C:2019:629.

- Demande de décision préjudicielle à la C.J.U.E présentée par la High Court (Irlande), Data Protection Commissioner / Facebook Ireland Limited, Maximilian Schrems, C-311/18, *J.O.U.E.*, C 249, du 16 juillet 2018, p. 15.

Juridictions belges

- Bruxelles nl. (18e ch.), 29 juin 2016, *J.L.M.B.*, 2017 (sommaire), liv. 26, p.1249.

- Civ. Bruxelles nl. (réf.), 9 novembre 2015, *J.L.M.B.*, 2017, liv. 26, p. 1240.

- Civ. Bruxelles nl. (24e ch.), 16 février 2018, *R.A.B.G.*, 2019, liv. 9, p. 695.

Autres juridictions

- TGI de Paris, 9 avril 2019, (disponible sur https://www.legalis.net/jurisprudences/tgi-de-paris-jugement-du-9-avril-2019/, dernière consultation le 06 août 2019).

- Royal Courts of Justice, Londres, 17 avril 2019, (disponible sur https://www.droit-technologie.org/wp-content/uploads/2019/05/954.pdf, dernière consultation le 06 août 2019).

Doctrine

- COTON F. et LIMBREE P., « 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 Le droit des MachinTech (FinTech, LegalTech, MedTech,…)*, Bruxelles, Larcier, 2018, pp. 9-78.

- DEJEMEPPE G., « L'affaire Facebook : questions de procédure », *R.D.T.I.*, 2016/1, n° 62, pp. 113-126.

- DELFORGE A., « Comment (ré)concilier RGPD et big data ? », *R.D.T.I.,* 2018/1, n° 70, pp. 15-29.

- DELFORGE A., « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *in Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Larcier, 2018, pp. 371-406.

- DE TERWANGNE C., « Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel », *in L'Europe des droits de l'homme à l'heure d'Internet*, Bruxelles, Bruylant, 2019, pp. 325-368.

- DOCQUIR B., « Chapitre 4. - Principes généraux de la protection des données », *in Droit du numérique*, Bruxelles, Larcier, 2018, pp. 415-457.

- FOSSOUL V., « L'identification par radiofréquence (RFID) : reflet des nouvelles tendances en matière de protection des données à caractère personnel », *in Le droit des nouvelles technologies et de l'internet*, Bruxelles, Bruylant, 2012, pp. 99-136.

- GAYREL C., « Chapitre 12. - L'expansion des standards européens de protection des données dans le monde », *in L'Europe des droits de l'homme à l'heure d'Internet*, Bruxelles, Bruylant, 2019, pp. 473-487.

- GROSJEAN A., « Chapitre 4 - Le profilage : un défi pour la protection des données à caractère personnel », *in Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, pp. 277-310.

- MICHAIL N., « Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union », *R.D.C.-T.B.H.*, 2019/1, pp. 52-79.

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

- PAILLER L., « Chapitre 1 - L'affaiblissement de la vie privée personnelle par le réseau social », *in Les réseaux sociaux sur internet et le droit au respect de la vie privée*, Bruxelles, Larcier, 2012, pp. 109-147.

- PONSART C. et ROBERT R., « Le règlement européen de protection des données personnelles », *J.T.*, 2018, pp. 421-438.

- POULLET Y., « Consentement et RGPD : des zones d'ombre ! », *D.C.C.R.*, 2019/1-2, n° 122-123, pp. 3-37.

- PUYRAIMOND J.-F., « L'intérêt légitime du responsable du traitement dans le RGPD : in cauda venenum ? », *D.C.C.R.*, 2019/1-2, n°122-123, pp. 39-77.

- RUE G., « Facebook doit changer ses conditions d'utilisation », *B.S.J.*, 2019/629, p. 11.

- STROWEL A., « Mutations des propriétés intellectuelles et du droit d'auteur à l'ère des données (data ownership, text and data mining, hyperlinking) », *A&M*, 2017/4, pp. 319-332.

- VAN CANNEYT T., « The general data protection regulation : 10 things company lawyers should know », *C.J.*, 2016/1, pp. 1-11.

Divers

Articles juridiques en ligne

- BINCTIN N., « Partie 2 : Créer une patrimonialité des données à droit constant », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles*, (Sous la direction de LÉGER L.), janvier 2018 (disponible sur https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf, dernière consultation le 06 août 2019), pp. 46-101.

- DEGRAVE E., *Facebook, les cookies et la justice belge : le retour,* le 22 mars 2018 (article en ligne disponible sur http://www.justice-en-ligne.be/article1044.html?utm_source=moteur_jel&utm_medium=thematique&utm_campaign=recherche, dernière consultation le 06 août 2019).

- DERIDDER T., *Affaire APD contre Facebook – la CJUE saisie !*, le 13 mai 2019 (article en ligne disponible sur https://equal-partners.eu/actualites/affaire-apd-contre-facebook-la-CJUE-saisie, dernière consultation le 06 août 2019).

- DOUCET B., « Avez-vous lu les conditions générales ? "GDPR, une occasion manquée ?"» *in Louvains mars-avril-mai 2018* (article en ligne disponible sur https://uclouvain.be/fr/decouvrir/louvains/avez-vous-lu-les-conditions-generales.html, dernière consultation le 06 août 2019).

- KOENIG G., « Introduction », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles*, (Sous la direction de LÉGER L.), janvier 2018 (disponible sur https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf, dernière consultation le 06 août 2019), pp. 12-19.

- LANDREAU I., LÉGER L. et PEZ-PÉRARD V., « Partie 1 : Les aspects socio-économiques et éthiques des données personnelles », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles*, (Sous la direction de LÉGER L.), janvier 2018 (disponible sur https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf, dernière consultation le 06 août 2019), pp. 20-45.

- VAN BRIEL D. et VAN DE MEULEBROUCKE A., *Commission vie privée devient Autorité de Protection des Données*, le 10 janvier 2018 (article en ligne disponible sur https://www.eubelius.com/fr/nouvelles/commission-vie-privee-devient-autorite-de-protection-des-donnees, dernière consultation le 06 août 2019).

- WALTER J.-P., *Le profilage des individus à l'heure du cyberespace: un défi pour le respect du droit à la protection des données*, 2009 (article en ligne disponible sur https://dokodoc.com/queue/le-profilage-des-individus-a-l-heure-du-cyberespace-un-defi-.html, dernière consultation le 06 août 2019)

- « Résumé », *in Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles*, (Sous la direction de LÉGER L.), janvier 2018 (disponible sur https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf, dernière consultation le 06 août 2019), p.8.

- Site officiel de la CNIL, *La publicité ciblée en ligne, communication présentée en séance plénière*, le 5 février 2009 (article en ligne disponible sur https://www.cnil.fr/sites/default/files/typo/document/Publicite_Ciblee_rapport_VD.pdf, dernière consultation le 06 août 2019).

- Site officiel de la CNIL, *Affaire Cambridge Analytica / Facebook*, le 12 avril 2018 (article en ligne disponible sur https://www.cnil.fr/fr/affaire-cambridge-analytica-facebook, dernière consultation le 06 août 2019).

- Site officiel de la CNIL, *La formation restreinte de la CNIL prononce une sanction de 50 millions d'euros à l'encontre de la société Google LLC*, le 21 janvier 2019 (article en ligne

disponible sur https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la, dernière consultation le 06 août 2019).

- Site officiel de l'APD Belge, *La Cour d'appel de Bruxelles réfère l'affaire Facebook à la Cour de justice de l'Union européenne*, le 8 mai 2019 (article en ligne disponible sur https://www.autoriteprotectiondonnees.be/news/la-cour-dappel-de-bruxelles-refere-laffaire-facebook-a-la-cour-de-justice-de-lunion, dernière consultation le 06 août 2019).

Interviews

- FRATI C., *Le RGPD a une génération de retard,* interview de Cyril PIERRE-BEAUSSE, Paperjam, le 22 mars 2018 (article en ligne disponible sur http://paperjam.lu/news/le-rgpd-a-une-generation-de-retard, dernière consultation le 06 août 2019).

- HOEBEKE D., « Avez-vous lu les conditions générales ? "If you are not paying, you are the product"», Interview de Anne-Lise SIBONY et Nikitas MICHAIL, *in Louvains mars-avril-mai 2018* (article en ligne disponible sur https://uclouvain.be/fr/decouvrir/louvains/avez-vous-lu-les-conditions-generales.html, dernière consultation le 06 août 2019).

- HOEBEKE D., « Avez-vous lu les conditions générales ? "Protéger les données... by design"», Interview de Olivier PEREIRA, *in Louvains mars-avril-mai 2018* (article en ligne disponible sur https://uclouvain.be/fr/decouvrir/louvains/avez-vous-lu-les-conditions-generales.html, dernière consultation le 06 août 2019).

- HOEBEKE D., « Avez-vous lu les conditions générales ? "Un droit fondamental"», Interview de Alain STROWEL, *in Louvains mars-avril-mai 2018* (article en ligne disponible sur https://uclouvain.be/fr/decouvrir/louvains/avez-vous-lu-les-conditions-generales.html, dernière consultation le 06 août 2019).

Communiqués de presse

- Communiqué de presse de la Commission Européenne, *À la demande de la Commission européenne et des autorités de protection des consommateurs, Facebook change ses conditions d'utilisation et précise l'utilisation des données fournies par les consommateurs*, le 9 avril 2019 (disponible sur http://europa.eu/rapid/press-release_IP-19-2048_fr.htm, dernière consultation le 06 août 2019).

Articles en ligne

- BATHELOT B., *Définition : Plugins sociaux Facebook*, Définitions Marketing, le 25 juillet 2015 (article en ligne disponible sur https://www.definitions-marketing.com/definition/plugins-sociaux-facebook/, dernière consultation le 06 août 2019).

- BOERO A., *Facebook : vers une amende de 5 milliards de dollars infligée aux USA*, Clubic, le 15 juillet 2019 (article en ligne disponible sur https://www.clubic.com/Internet/facebook/actualite-863927-facebook-amende-5-dollars-infligee-usa.html, dernière consultation le 06 août 2019).

- CADWALLADR C. et GRAHAM-HARRISON E., *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, The Guardian, le 17 mars 2018 (article en ligne disponible sur https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election, dernière consultation le 06 août 2019).

- CONSTINE J., *'Facebook Rewards' QR codes dangle discounts for offline purchases*, Techcrunch, 2017 (article en ligne disponible sur https://techcrunch.com/2017/05/01/facebook-rewards/, dernière consultation le 06 août 2019).

- L. B., *Les sous-traitants de Facebook lisent vos posts privés pour entraîner l'IA*, Le Big Data, le 6 mai 2019 (article en ligne disponible sur https://www.lebigdata.fr/sous-traitants-facebook-posts-prives, dernière consultation le 06 août 2019).

- LE GUENNO M., *Facebook étend sa régie publicitaire à tout le Web, y compris les non-membres*, Influenth, le 28 mai 2016 (article en ligne disponible sur http://www.influenth.com/facebook-regie-publicitaire/, dernière consultation le 06 août 2019).

- MABILLE P., *Si c'est gratuit, c'est que vous êtes le produi*t, La Tribune, le 10 avril 2018 (article en ligne disponible sur https://www.latribune.fr/opinions/editos/si-c-est-gratuit-c-est-que-vous-etes-le-produit-774672.html, dernière consultation le 06 août 2019).

- PERRIN A., *Americans are changing their relationship with Facebook*, Pew Research Center, le 5 septembre 2018 (article en ligne disponible sur http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/, dernière consultation le 06 août 2019).

- PROTALINSKI E., *Facebook completes move from Palo Alto to Menlo Park*, ZDNET, le 19 décembre 2011 (article en ligne disponible sur https://www.zdnet.com/article/facebook-completes-move-from-palo-alto-to-menlo-park/, dernière consultation le 06 août 2019).

- RAHMIL D.-J., *Vous ne contrôlez qu'un tiers de votre identité en ligne*, L'ADN, le 13 février 2019 (article en ligne disponible sur https://www.ladn.eu/tech-a-suivre/data-comment-construit-identite-ligne/, dernière consultation le 06 août 2019).

- SZADKOWSKI M., *Facebook donne un peu plus de détails sur le ciblage publicitaire de ses utilisateurs*, Le Monde, le 12 juillet 2019 (article en ligne disponible sur https://www.lemonde.fr/pixels/article/2019/07/12/facebook-donne-un-peu-plus-de-detail-sur-le-ciblage-publicitaire-de-ses-utilisateurs_5488626_4408996.html?utm_medium=Social&utm_source=Facebook&fbclid=IwAR3WAtN26v5iXjasaiI1yWvARUhW5qoC35Z44O25IMbkHoC6E1L4kMPgNzE#Echobox=1562947577, dernière consultation le 06 août 2019).

- SZYMIELEWICZ K., *Your digital identity has three layers, and you can only protect one of them*, Quartz, le 25 janvier 2019 (article en ligne disponible sur https://qz.com/1525661/your-digital-

identity-has-three-layers-and-you-can-only-protect-one-of-them/, dernière consultation le 06 août 2019).

- *Adieu Big Data, bonjour Smart Data !*, E-marketing, le 29 juin 2018 (article en ligne disponible sur https://www.e-marketing.fr/Thematique/data-1091/breve/adieu-big-data-bonjour-smart-data-332456.htm, dernière consultation le 06 août 2019).

- *Amende record pour Facebook : "Une centralisation des données personnelles sans équivalent à l'échelle de la planète"*, Franceinfo, le 13 juillet 2019 (article en ligne disponible sur https://www.francetvinfo.fr/Internet/reseaux-sociaux/facebook/amende-record-pour-facebook-une-centralisation-des-donnees-personnelles-sans-equivalent-a-l-echelle-de-la-planete_3534451.html, dernière consultation le 06 août 2019).

- *Si c'est gratuit, vous êtes le produit*, Adesias, 2013 (article en ligne disponible sur https://adesias.fr/animation/adesias-si-c-est-gratuit-vous-êtes-le-produit/-u658, dernière consultation le 06 août 2019).

- *Smart Data*, E-marketing Glossaire (article en ligne disponible sur https://www.e-marketing.fr/definitions-glossaire/smart-data-254969.htm, dernière consultation le 06 août 2019).

Publications de Facebook et liens vers le réseau social

- Facebook, *Addenda concernant le responsable de traitement des données Statistiques* (disponible sur https://www.facebook.com/legal/terms/page_controller_addendum, dernière consultation le 06 août 2019).

- Facebook, *Sélectionner une langue* (disponible sur https://m.facebook.com/language.php, dernière consultation le 06 août 2019).

- Facebook Business, *Publicités Facebook, Entrez en contact avec de futurs clients et fans* (disponible sur https://www.facebook.com/business/ads, dernière consultation le 06 août 2019).

- Facebook Business, *Qu'est-ce que le Règlement général sur la protection des données (RGPD)* ? (disponible sur https://www.facebook.com/business/gdpr, dernière consultation le 06 août 2019).

- Facebook Newsroom, *Company Info* (disponible sur https://newsroom.fb.com/company-info/, dernière consultation le 06 août 2019).

- Facebook Newsroom, *Facebook to Establish International Headquarters in Dublin, Ireland*, le 2 octobre 2008 (article disponible sur https://newsroom.fb.com/news/2008/10/facebook-to-establish-international-headquarters-in-dublin-ireland/, dernière consultation le 06 août 2019).

- Facebook Research, *Facebook's Top Open Data Problems*, by J. WIENER and N. BRONSON, le 22 octobre 2014 (article disponible sur https://research.fb.com/blog/2014/10/facebook-s-top-open-data-problems/, dernière consultation le 06 août 2019).

Sites internet

- Fiche d'entreprise de Facebook Ireland (disponible sur https://www.societe.com/societe/facebook-ireland-limited-814665519.html dernière consultation le 06 août 2019).

- GDPR Enforcement Tracker de la CMS (disponible sur http://www.enforcementtracker.com, dernière consultation le 06 août 2019).

- Privacy Shield Framework, Facebook Inc. Participation (disponible sur https://www.privacyshield.gov/participant?id=a2zt0000000GnywAAC, dernière consultation le 06 août 2019).

Autres

- BERRY M. et LINOFF G., *Data Mining Techniques: For Marketing, Sales, and Customer Relationship Management (second edition)*, Indianapolis, Wiley Publishing Inc, 2004.

- TUFFERY S., *Data mining et statistique décisionnelle, l'intelligence dans les bases de données*, Paris, Technip, 2010. (voir Bespo QA 76 .9.D343 T 247899).

- Le Petit Larousse illustré grand format, édition 2013.

LOUVAIN-LA-NEUVE | BRUXELLES | MONS | TOURNAI | CHARLEROI | NAMUR
Place Montesquieu, 2 bte L2.07.01, 1348 Louvain-la-Neuve, Belgique | **www.uclouvain.be/drt**