

Faculté de droit et de criminologie

La publicité ciblée : un défi pour la protection des données à caractère personnel

Analyse d'un cas pratique : le ciblage publicitaire opéré par Facebook au regard des exigences imposées par le Règlement Général sur la Protection des Données

Auteur : **Marie-Emmanuelle RODRIGUEZ**

Promoteur : **François JONGEN**

Année académique : **2019-2020**

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.

* À ce sujet, voy. notamment **<http://www.uclouvain.be/plagiat>**.

REMERCIEMENTS

Mes remerciements vont à toutes les personnes qui m'ont aidée dans la réalisation de ce mémoire. Qu'elles trouvent ici l'expression de ma plus sincère reconnaissance.

J'adresse une pensée particulière à mon promoteur, le Professeur F. JONGEN, pour sa disponibilité et ses conseils avisés.

Je tiens également à remercier chaleureusement mon père, E. RODRIGUEZ, ma mère, K. FOUREZ et ma petite sœur, M. RODRIGUEZ, pour le soutien indéfectible qu'ils m'ont apporté tout au long de mon parcours universitaire.

Enfin, mes derniers remerciements s'adressent à M. STERN, pour son aide précieuse, ainsi qu'à N. WAUTHIER et à chacun de mes amis, sans qui la vie n'aurait pas la même saveur.

TABLE DES MATIÈRES

Introduction.....	1
Titre 1. Mise en contexte théorique	4
Chapitre 1. Définition des principaux concepts.....	4
Section 1. Le droit à la protection des données à caractère personnel : avant-propos succinct	4
Section 2. Le profilage.....	5
§1. Tentative de délimitation de la notion	5
§2. Finalités poursuivies	5
Section 3. La publicité ciblée.....	7
Chapitre 2. Les étapes du profilage publicitaire	10
Section 1. Considérations préliminaires	10
Section 2. La collecte des données	11
§1. Déroulement.....	11
§2. Principaux outils de collecte d'informations	12
Section 2. L'analyse des données, ou « <i>data mining</i> »	13
Section 3. L'application des données à un profil, ou « <i>inférence</i> »	15
Section 4. Le profilage aux fins de publicité ciblée en ligne constitue-t-il un traitement de données à caractère personnel ?	16
Chapitre 3. Les principaux risques du profilage	17
Titre 2. La publicité ciblée opérée par Facebook.....	20
Chapitre 1. L'applicabilité du RGPD à Facebook	21
Section 1. Considérations préliminaires	21
§1. Quelques notions élémentaires à propos de Facebook	21
§2. Le rôle du RGPD dans le paysage législatif	22
Section 2. Champ d'application.....	23
§1. Champ d'application matériel.....	23
A. Un « traitement ».....	24
B. De « données à caractère personnel »	24
§2. Champ d'application personnel	25
A. Le responsable de traitement.....	26
B. L'hypothèse de la responsabilité conjointe	27
C. Le sous-traitant, et sa relation avec le responsable de traitement	28

§3. Champ d'application territorial.....	29
A. La localisation de l'établissement.....	29
B. Le cas d'un établissement situé sur le territoire de l'Union.....	30
C. Le cas d'un établissement situé en dehors du territoire de l'Union	32
Chapitre 2. Les exigences imposées par le RGPD.....	32
Section 1. Les conditions de licéité du traitement	32
§1. Le consentement	33
§2. L'intérêt légitime	35
Section 2. Les principes de base relatifs au traitement de données à caractère personnel ..	37
§1. Principes de licéité, de loyauté et de transparence du traitement	37
§2. Principe de limitation des finalités.....	38
§3. Principe de minimisation des données.....	39
§4. Principe d'exactitude des données	40
§5. Principe de limitation de la conservation.....	40
§6. Principe d'intégrité et de confidentialité des données	41
§7. Principe de responsabilité ("accountability")	41
Section 3. Les obligations du responsable de traitement	42
§1. Mise en pratique du principe de responsabilité ("accountability").....	42
§2. Deux obligations pour tout traitement : le "privacy by design" et le "privacy by default"	43
A. "Privacy by design"	44
B. "Privacy by default"	45
Titre 3. Mieux protéger ses données sur Internet.....	48
Chapitre 1. Une meilleure sensibilisation des individus.....	48
Section 1. Aperçu de quelques actions préventives possibles	48
§1. Campagnes de sensibilisation et outils pédagogiques	48
§2. Configuration du navigateur, destructeur de cookies et bloqueur de publicité.....	49
§3. Anonymat et pseudonymat	50
A. Données anonymisées : une garantie suffisante ?.....	50
B. Données pseudonymisées : un outil efficace ?.....	51
Section 2. L'information, l'éducation et la responsabilisation des internautes	52
Chapitre 2. Les alternatives envisageables propres à Facebook	54
Section 1. La possibilité de monétiser ses données	55
Section 2. La possibilité de payer le service, ou le « prix de la <i>privacy</i> »	56

Conclusion	58
BIBLIOGRAPHIE.....	61
ANNEXES. Retranscription des interviews	72
Interview n° 1. François Zöfel, Data Protection Officer – 23 juillet 2020	72
Interview n° 2. Frédérique Meurice, Head of Digital Service Design – 30 juillet 2020	76

Introduction

Tout a commencé par le rêve d'un monde interconnecté. Un endroit qui permettrait à chacun de vivre une multitude d'expériences en ligne : partager des moments de vie par le biais de photos et de vidéos ; échanger des messages pour maintenir le contact avec ses proches ou pour construire de nouvelles relations ; rejoindre ou créer des groupes d'intérêts communs dans de nombreuses sphères telles que l'université, le sport, ou encore la musique ; mais également débattre des sujets d'actualité, partager un regard critique sur le monde, soutenir des causes contemporaines, etc.¹

En quelques années, Facebook est devenu un réseau social à échelle internationale, jusqu'à atteindre les 2,7 milliards d'utilisateurs actifs aux quatre coins de la planète². Ce sont autant de membres qui laissent, au cours de leur navigation, un nombre incalculable d'empreintes numériques, lesquelles alimentent une industrie qui brasse des milliers de milliards de dollars chaque année. Une part importante des revenus générés par la société américaine provient d'ailleurs de la publicité diffusée sur la plateforme ; publicité qui est, la plupart du temps, offerte aux consommateurs de manière ciblée.

Toutefois, ce business n'est pas sans risque. L'idée d'une connexion gratuite était tellement attractive pour les internautes, qu'aucun d'entre eux n'a pris la peine de lire les conditions générales. La vérité qui se cache derrière Facebook laisse sans voix : si c'est gratuit, c'est parce que c'est l'utilisateur lui-même qui est le produit³. Car il ne faut pas l'oublier, les géants du Web⁴ sont avant tout des sociétés privées qui ont pour objectif de rentabiliser les données à caractère personnel récoltées à propos de leurs membres.

Ainsi, l'ensemble des interactions de l'individu, de ses paiements par carte, à sa localisation, en passant par ses *likes*, est récolté en temps réel, pour être rattaché à son profil,

¹ La mission du réseau social est d'ailleurs décrite comme suit : *“Give people the power to build community and bring the world closer together”*. Voy. en ce sens Facebook, *À propos* (disponible sur https://www.facebook.com/pg/facebook/about/?ref=page_internal, page consultée le 8 août 2020).

² JOURNAL DU NET, *Nombre d'utilisateurs de Facebook dans le monde*, 31 juillet 2020 (disponible sur <https://www.journaldunet.com/ebusiness/le-net/1125265-nombre-d-utilisateurs-de-facebook-dans-le-monde/>, page consultée le 8 août 2020).

³ MR MONDIALISATION, *De Google à Facebook : « si c'est gratuit, vous êtes le produit »*, 7 mai 2016 (disponible sur <https://mrmondialisation.org/google-facebook-gratuit-vous-etes-produit/>, page consultée le 8 août 2020).

⁴ Les géants du Web sont plus couramment regroupés sous l'acronyme « GAFAP » (Google – Amazon – Facebook – Apple).

dans le but final d'attirer son attention avec du contenu uniquement visible par lui, et spécifiquement conçu pour lui. La violation de la privacité du consommateur s'opère sous ses yeux, et avec sa collaboration, ce dernier fournissant en toute innocence (ou indifférence) toutes les informations nécessaires à la marchandisation de ses données.

Plus que jamais, la protection de la vie privée et des données à caractère personnel, deux libertés fondamentales considérées comme essentielles dans un État de droit, est menacée par l'appât du gain des publicitaires. En ce sens, la publicité ciblée opérée par Facebook a retenu toute notre attention, le choix du réseau social nous apparaissant légitime de par son nombre élevé d'utilisateurs et son influence non-négligeable sur le marché numérique. Parmi la multiplicité des sources de droit applicable au cas d'espèce, nous avons décidé de nous focaliser sur le Règlement Général de la Protection des Données (ci-après « RGPD »⁵ ou « le règlement »), dont l'adoption le 25 mai 2018 a fait énormément de bruit dans l'Union européenne, mais également dans le reste du monde⁶.

Le présent mémoire propose une étude de la problématique qui se décline en trois Titres.

Dans un premier Titre, nous aborderons les fondements théoriques indispensables à la bonne compréhension du sujet et ce, en trois chapitres. Premièrement, nous définirons les principaux concepts tels que le droit à la protection des données à caractère personnel, le profilage et la publicité ciblée. Deuxièmement, nous décortiquerons les différentes étapes du profilage publicitaire. Enfin, nous clôturerons la mise en contexte avec un dernier chapitre relatifs aux principaux risques du profilage.

Dans un deuxième Titre, nous analyserons la publicité ciblée opérée par Facebook, à la lumière du règlement européen. En toute logique, nous entrerons dans le vif du sujet en vérifiant d'abord l'applicabilité du texte à la multinationale, eu égard aux champs d'application *ratione materiae*, *ratione personae* et *ratione loci*. Ce n'est qu'une fois la vérification établie que nous nous pencherons sur les exigences imposées par le RGPD.

⁵ Ou « *GDPR* », en anglais.

⁶ 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.

Enfin, dans un troisième et dernier Titre, nous nous intéresserons de plus près à la façon dont il conviendrait de mettre en place une meilleure protection des données personnelles, en exposant diverses pistes de solutions ainsi que quelques perspectives d'avenir.

Que le lecteur soit d'emblée averti : si la protection des données à caractère personnel et le ciblage publicitaire sont deux thématiques très vastes, la mise en corrélation de celles-ci l'est d'autant plus. Sans prétendre à l'exhaustivité, ce mémoire se borne à présenter une critique du phénomène prédécrit sous un angle juridique, après avoir regroupé le plus de contributions doctrinales et jurisprudentielles possibles. Les positions qu'adopte cette étude n'engagent que leur auteur.

Titre 1. Mise en contexte théorique

Chapitre 1. Définition des principaux concepts

Section 1. Le droit à la protection des données à caractère personnel : avant-propos succinct

Longtemps considérée comme faisant partie du droit au respect de la vie privée⁷, faisant ensuite timidement son entrée en tant que nouveau concept de vie privée connu sous l'appellation de « *droit à l'autodétermination informationnelle* »⁸, la protection des données a finalement réussi à se forger une place au fil des années sur la scène européenne, jusqu'à devenir une notion à part entière.

Désormais reconnu comme un droit fondamental dans l'ordre juridique de l'UE⁹, le droit à la protection des données à caractère personnel¹⁰ continue malgré tout d'entretenir une relation de proximité avec le droit au respect de la vie privée, bien qu'il subsiste de notables différences entre les deux concepts¹¹.

Tous deux étroitement liés quant aux valeurs similaires qu'ils protègent, à savoir l'autonomie et la dignité humaine des individus, ces deux droits se distinguent toutefois par leur formulation et leur portée¹². En effet, alors que le droit au respect de la vie privée est

⁷ N. RAGHENO, « Droits fondamentaux et société numérique : la vie privée existe-t-elle encore ? » in *Data protection & privacy : le GDPR dans la pratique*, Limal, Anthemis, 2017, p. 18.

⁸ Dans un arrêt de 2017, la Cour européenne des Droits de l'Homme (ci-après « Cour eur. D.H. »), reconnaît pour la première fois que l'article 8 de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales (ci-après « CEDH ») consacre « *le droit à une forme d'auto-détermination informationnelle* ». Voy. en ce sens Cour eur. D.H., arrêt *Satakunnan Markkinapörssi Oy et Satamedia Oy contre Finlande*, 27 juin 2017, req. n° 931/13, § 137.

⁹ Voy. notamment Charte des Droits Fondamentaux de l'Union Européenne, *J.O.U.E.*, C 326, 26 octobre 2012, p. 391, art. 8.

¹⁰ En ce qui concerne la notion de « *données à caractère personnel* », on renvoie aux développements du Titre 2, Chapitre, 1, Section 2, § 1 sur le champ d'application *ratione materiae* de Facebook.

¹¹ AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, Édition 2018, Luxembourg, Office des publications de l'Union européenne, 2019, p. 20.

¹² AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, *op. cit.*, pp. 21-22.

décrit comme une interdiction *générale* de toute ingérence¹³, le droit à la protection des données à caractère personnel se veut beaucoup plus *circonscrit*, et se limite à l'appréciation de la légalité des traitements des données à caractère personnel¹⁴.

Section 2. Le profilage

§1. Tentative de délimitation de la notion

Conformément aux articles 4, 4) du RGPD et 3, § 4 de la Directive (UE) 2016/680¹⁵, le profilage désigne « *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* ». Cette définition, très large, englobe notamment la publicité ciblée¹⁶.

On précise toutefois qu'il reste extrêmement difficile de délimiter les contours exacts du profilage, tant le processus regroupe d'innombrables techniques, reposant elles-mêmes sur de multiples technologies complexes à appréhender car en constante évolution¹⁷.

§2. Finalités poursuivies

Les pratiques de profilage sont notamment utilisées pour générer des connaissances, en analysant des données préalablement récoltées, afin de formuler des hypothèses sur un

¹³ À moins que l'ingérence ne soit prévue par la loi, poursuive des intérêts publics importants et légitimes et soit nécessaire dans une société démocratique, comme le prescrit l'article 8 de la CEDH.

¹⁴ AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE, *Guide pour la prévention du profilage illicite aujourd'hui et demain*, Luxembourg, Office des publications de l'Union européenne, 2019, pp. 36-37.

¹⁵ Directive (UE) n° 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *J.O.U.E.*, L. 119/89, 4 mai 2016.

¹⁶ C. DE TERWANGNE, K. ROSIER et B. LOSDYCK, « Le règlement européen relatif à la protection des données à caractère personnel : quelles nouveautés ? », *J.D.E.*, 2017/8, p. 313.

¹⁷ 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. 291.

individu¹⁸. Une fois le processus abouti, le profilage permet alors « *de tracer les internautes dans le temps et sur différents sites, de créer des profils très précis de leurs goûts selon leurs caractéristiques, et d’afficher en ligne les publicités qui reflètent leurs intérêts* »¹⁹.

Même s’il est vrai que dans la plupart des cas, le profilage va de pair avec le suivi des internautes²⁰, il faut garder à l’esprit que le profilage n’est pas « *une finalité en soi* »²¹, postulat qui est d’ailleurs appuyé par la diversité de ses objectifs dans de nombreux secteurs d’activités, relevant tant du secteur public que du secteur privé²².

À titre d’illustration, on retrouve parmi les principales applications du profilage : la lutte contre la criminalité (les agents de police ayant régulièrement et légitimement recours à ce processus afin de traiter les infractions pénales déjà commises et de prévenir celles à venir)²³, la lutte contre la fraude fiscale (le profilage se montrant utile dans le repérage des fraudeurs et dans la mise en place de contrôles plus efficaces par l’État)²⁴, l’analyse de solvabilité et de prédiction de l’état de santé effectuée par les compagnies d’assurance (dans le but d’éviter les mauvais payeurs et dès lors, d’accepter ou de refuser l’octroi d’un crédit)²⁵, etc.

Par conséquent, on remarque que le profilage peut servir l’intérêt général et se montrer bénéfique à la société dans son ensemble²⁶, comme le souhaitait déjà le RGPD en proclamant que « *le traitement des données à caractère personnel devrait être conçu pour servir l’humanité* »²⁷.

¹⁸ Pour de plus amples informations sur les étapes du profilage, voy. la Section 2 de ce chapitre.

¹⁹ A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 279.

²⁰ 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.

²¹ J.-P. WALTER, *Le profilage des individus à l’heure du cyberspace : un défi pour le respect du droit à la protection des données*, 2009 (disponible sur <https://dokodoc.com/queue/le-profilage-des-individus-a-l-heure-du-cyberspace-un-defi-.html>, page consultée le 10 juillet 2020), p. 8.

²² *Ibid.*, pp. 16-17.

²³ AGENCE DES DROITS FONDAMENTAUX DE L’UNION EUROPEENNE, *Guide pour la prévention du profilage illicite aujourd’hui et demain*, *op. cit.*, p. 20.

²⁴ A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 286.

²⁵ J.-P. WALTER, *Le profilage des individus à l’heure du cyberspace : un défi pour le respect du droit à la protection des données*, *op. cit.*, p. 17.

²⁶ A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 280.

²⁷ RGPD, considérant n° 4.

Au surplus, les pratiques de profilage ne sont pas dénuées d'avantages pour les consommateurs, en ce qu'elles façonnent l'offre qui leur est proposée en fonction de leurs intérêts et préférences²⁸.

Toutefois, aux yeux de nombreuses entreprises, les techniques de profilage représentent surtout un intérêt économique considérable et sont principalement utilisées 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)* »²⁹.

En réalité, rares sont les internautes à n'avoir jamais vécu l'expérience suivante : après avoir réservé ses vacances de rêve en ligne et acheté son billet d'avion pour la Californie, Monsieur X. *scrolle*³⁰ le fil d'actualité de son réseau social préféré et voit s'afficher des publicités pour une location de voiture aux États-Unis, pour une excursion guidée au parc national de Yosemite ou pour diverses autres offres plus ou moins attractives en lien avec son prochain voyage³¹. Loin d'être une coïncidence, l'internaute a fait les frais du profilage, processus ayant abouti à lui proposer des publicités ciblées en fonction de ses clics sur Internet. Le ciblage publicitaire est ainsi l'aspect du profilage qui retiendra toute notre attention.

Section 3. La publicité ciblée

Bien que la publicité ciblée ne soit pas définie en tant que telle par la loi, le droit européen définit la « *communication commerciale* » comme « *toute forme de communication destinée à promouvoir, directement ou indirectement, des biens, des services, ou l'image d'une entreprise, d'une organisation ou d'une personne ayant une activité commerciale,*

²⁸ 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.

²⁹ J.-P. WALTER, *Le profilage des individus à l'heure du cyberspace : un défi pour le respect du droit à la protection des données*, op. cit., p. 17.

³⁰ Cet anglicisme désigne le fait de faire défiler un contenu sur un écran informatique.

³¹ COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES (CNIL), *La publicité ciblée en ligne, communication présentée en séance plénière*, 5 février 2009 (disponible sur http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/Publicite_Ciblee_rapport_VD.pdf, page consultée le 5 juillet 2020), p. 4.

industrielle, artisanale ou exerçant une profession réglementée »³². Le droit belge nous offre la même définition de la « *publicité* », ni plus large ni plus étroite, et vise par conséquent le même champ d'application³³.

Il existe trois types de publicité ciblée en ligne : la « *publicité personnalisée* », la « *publicité contextuelle* » et la « *publicité comportementale* ».

La publicité personnalisée « *classique* », parfois également connue sous l'appellation de « *publicité personnelle* »³⁴ ou de « *publicité segmentée* »³⁵, est sélectionnée sur base des caractéristiques connues de l'utilisateur (telles que l'âge, le sexe, les coordonnées, etc.) qu'il a lui-même renseignées, notamment au moment de s'inscrire sur un service³⁶. Considérée comme la forme de publicité la plus traditionnelle, elle est aujourd'hui revisitée par les réseaux sociaux, qui jouissent désormais d'un ensemble détaillé de données personnelles à propos de leurs utilisateurs³⁷. En effet, bien plus que les éléments classiques qui composent leur identité, les internautes partagent dorénavant leurs centres d'intérêts et leurs passions, ce qui permet aux plateformes de mettre au point des publicités personnalisées très pointues³⁸.

La publicité personnalisée est soumise à la réglementation relative à la protection des données en ce qu'elle nécessite l'identification d'un individu précis, ce qui n'est pas le cas des autres types de publicités ciblées, qui requièrent plutôt la constitution de profils de consommation plus ou moins aboutis suivant la technique utilisée, et seront ainsi confrontées à quelques difficultés quant à l'application des règles normatives en question³⁹.

³² Directive (CE) n° 2000/31 du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »), *J.O.U.E.*, L. 178, 17 juillet 2000, art. 2, f).

³³ Code de droit économique, art. I.18, 6°.

³⁴ L. VOGEL et J. VOGEL, « I. - Publicité sur Internet » in *Traité de droit économique – Tome 3 : Droit de la consommation*, Bruxelles, Bruylant, 2017, p. 161.

³⁵ GROUPE DE TRAVAIL « ARTICLE 29 », Avis 2/2010 sur la publicité comportementale en ligne, WP 171, 22 juin 2010, (00909/10/FR), p. 5.

³⁶ A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 288.

³⁷ COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES (CNIL), *La publicité ciblée en ligne, communication présentée en séance plénière*, *op. cit.*, p. 5.

³⁸ *Ibid.*

³⁹ L. VOGEL et J. VOGEL, « I. - Publicité sur Internet », *op. cit.*, p. 170. Nous reviendrons toutefois sur ce point dans le Chapitre 2, Section 4, relatif à la question de savoir si le profilage aux fins de publicité ciblée en ligne constitue un traitement de données « à caractère personnel ».

La publicité contextuelle est quant à elle choisie « *soit en fonction du contenu textuel de la page Web dans laquelle la publicité est insérée, soit, s'il s'agit d'un moteur de recherche, en fonction du mot-clé utilisé par l'internaute pendant sa recherche* »⁴⁰. Ces données peuvent parfois être complétées par « *des informations de géolocalisation déduites de l'adresse IP de l'internaute, ou par la précédente requête dans le cas particulier d'un moteur de recherche* »⁴¹. La publicité est ainsi ciblée sur base des centres d'intérêts présumés de l'utilisateur : par exemple, des publicités présentant des articles pour bébé s'afficheront sur un site dédié aux jeunes parents⁴².

Enfin, la publicité comportementale repose sur l'étude du comportement des individus à travers le temps⁴³. Plus précisément, elle vise à observer les caractéristiques du comportement de l'internaute par le biais de ses actions (visites de sites, pages consultées, interactions, préférences exprimées sur les réseaux sociaux⁴⁴, mots-clés, requêtes formulées sur moteurs de recherches, production de contenus en ligne, *chats*, etc.)⁴⁵ pour lui construire un profil sur-mesure et lui soumettre des publicités adaptées⁴⁶.

Alors que publicités personnalisée et conceptuelle s'appuient sur des faits instantanés, à savoir les agissements d'un utilisateur sur un site Web particulier, la publicité comportementale offre l'avantage d'amener un plan très détaillé de la vie en ligne de l'internaute dans son ensemble, en révélant « *un grand nombre des sites web et des pages spécifiques consultés, combien de temps certains articles ou éléments ont été regardés, dans quel ordre, etc.* »⁴⁷

⁴⁰ A. GROSJEAN, « Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 288.

⁴¹ COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES (CNIL), *La publicité ciblée en ligne*, *op. cit.*, p. 5.

⁴² L. VOGEL et J. VOGEL, « I. - Publicité sur Internet », *op. cit.*, p. 170.

⁴³ A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 288.

⁴⁴ Par exemple grâce aux « *likes* » sur Facebook.

⁴⁵ L. VOGEL et J. VOGEL, « I. - Publicité sur Internet », *op. cit.*, pp. 169-170.

⁴⁶ GROUPE DE TRAVAIL « ARTICLE 29 », Avis 2/2010 sur la publicité comportementale en ligne, *op. cit.*, p. 5.

⁴⁷ GROUPE DE TRAVAIL « ARTICLE 29 », Avis 2/2010 sur la publicité comportementale en ligne, *op. cit.*, p. 5.

Chapitre 2. Les étapes du profilage publicitaire

Le profilage se compose de trois grandes étapes : premièrement, la collecte à grande échelle de données personnelles relatives au comportement des individus ; deuxièmement, l'analyse des données préalablement collectées aux fins d'établir des corrélations entre certaines données et certains comportements ; enfin, la troisième et dernière étape vise à appliquer un profil à un individu⁴⁸.

Section 1. Considérations préliminaires

Avant d'entrer dans de plus amples développements, il convient de distinguer deux types de profilage : le « *profilage abstrait* », qui repose sur des données qui n'appartiennent généralement pas à la personne concernée, et qui débouche sur un profil de groupe ; et le « *profilage individuel* » (parfois également appelé « *profilage spécifique* »), qui repose cette fois-ci sur l'assemblage de données propres à la personne concernée, et qui débouche par conséquent sur un profil individuel⁴⁹.

Les auteurs du rapport sur l'application de la Convention 108 au mécanisme du profilage ajoutent que le profilage abstrait s'appuie sur « *la mise en évidence d'informations, l'établissement de prédictions et finalement l'inférence* »⁵⁰, tandis que le profilage spécifique est « *généré uniquement sur la base de la collecte et l'analyse de données relatives à la personne concernée, sans inférence ou prédiction issue de sources externes* »⁵¹.

Par conséquent, les développements relatifs aux différentes étapes du processus qui suivront n'ont vocation à s'appliquer que dans le cadre du profilage abstrait⁵².

⁴⁸ FOSSOUL V., « L'identification par radiofréquence (RFID) : reflet des nouvelles tendances en matière de protection des données à caractère personnel », *op. cit.*, pp. 128-129.

⁴⁹ J.-P. WALTER, *Le profilage des individus à l'heure du cyberspace : un défi pour le respect du droit à la protection des données*, *op. cit.*, pp. 8-9.

⁵⁰ J.-M. DINANT, C. LAZARO, Y. POULLET, N. LEFEVER et A. ROUVROY, *L'application de la Convention 108 au mécanisme de profilage – Éléments de réflexion destinés au travail du futur Comité consultatif (T-PD)*, 11 janvier 2008 (disponible sur <https://www.coe.int/fr/web/data-protection/reports-studies-and-opinions>, page consultée le 15 mai 2020), p. 3.

⁵¹ *Ibid.*

⁵² Il est tout de même intéressant de préciser qu'en pratique, les profils abstraits sont régulièrement générés, en partie du moins, à partir de profils spécifiques, et vice versa. Voy. en ce sens J.-M. DINANT, C. LAZARO, Y. POULLET, N. LEFEVER et A. ROUVROY, *L'application de la Convention 108 au mécanisme de profilage – Éléments de réflexion destinés au travail du futur Comité consultatif (T-PD)*, *op. cit.*, p. 3.

Section 2. La collecte des données

§1. Déroulement

La première étape consiste à collecter des informations, « *par le regroupement de données à caractère personnel ou de données anonymes* »⁵³. S'il s'avère que les données concernent une personne identifiée ou identifiable, elles seront généralement anonymisées lors de cette étape, car l'observation du comportement et des caractéristiques ne requiert pas que la personne soit identifiée ou identifiable⁵⁴.

En outre, l'origine des données n'a pas d'importance, elles peuvent être internes (par exemple, une banque pourrait rédiger une liste anonyme de ses clients à découvert et de leurs caractéristiques) ou externes (par exemple, une entreprise de marketing pourrait solliciter la liste des « *paniers d'achats* » d'une grande chaîne de supermarché, sans identification des consommateurs en question)⁵⁵.

La construction d'une publicité ciblée de qualité nécessite de récolter un maximum d'informations sur l'internaute⁵⁶. C'est ce qui explique pourquoi une société comme Facebook, qui offre un service gratuit (ou tout du moins en apparence, car en réalité, ce service est en grande partie financée par la publicité) se doit de diversifier les services et les activités qu'elle propose, afin de collecter toujours plus d'informations sur le comportement de ses utilisateurs⁵⁷. Ainsi, pour l'individu qui s'en soucierait, il est désormais devenu extrêmement difficile, voire quasiment impossible, d'échapper totalement à la collecte de ses données personnelles⁵⁸.

⁵³ A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 292.

⁵⁴ *Ibid.*

⁵⁵ J.-M. DINANT, C. LAZARO, Y. POULLET, N. LEFEVER et A. ROUVROY, *L'application de la Convention 108 au mécanisme de profilage – Éléments de réflexion destinés au travail du futur Comité consultatif (T-PD)*, *op. cit.*, p. 3.

⁵⁶ L. VOGEL et J. VOGEL, « I. - Publicité sur Internet », *op. cit.*, p. 161.

⁵⁷ J.-P. WALTER, *Le profilage des individus à l'heure du cyberspace : un défi pour le respect du droit à la protection des données*, *op. cit.*, p. 3.

⁵⁸ R. TINIERE, « Article 8. - Protection des données à caractère personnel », in *Charte des droits fondamentaux de l'Union européenne*, Bruxelles, Bruylant, 2017, p. 214.

§2. Principaux outils de collecte d'informations

Il existe de très nombreuses méthodes qui offrent la possibilité aux réseaux publicitaires de collecter des informations supplémentaires sur l'utilisateur⁵⁹, qu'elles soient explicites (lorsque l'internaute renseigne lui-même certaines informations) ou implicites (lorsque les informations sont collectées à l'insu de l'individu)⁶⁰. Loin de nous l'idée d'en dresser une liste exhaustive, nous nous concentrerons uniquement sur les plus courantes d'entre elles.

Les méthodes explicites de collecte de données consistent simplement à faire compléter à l'internaute des formulaires de renseignements ou des questionnaires en ligne⁶¹. Par exemple, l'utilisateur de Facebook renseigne sur son profil son nom, son prénom et sa date de naissance, mais également son emploi, son parcours scolaire, sa ville de résidence actuelle ou sa ville d'origine, ses centres d'intérêts, ses croyances religieuses, ses opinions politiques, son numéro de téléphone, les langues qu'il parle et même le statut de sa relation amoureuse⁶².

Les techniques implicites de collecte de données sont quant à elles plus subtiles mais surtout plus dangereuses, car elles espionnent l'internaute dans ses moindres clics, la plupart du temps sans que ce dernier en ait conscience⁶³.

Au premier plan des outils qui peuvent s'avérer menaçants pour la protection de la vie privée, on retrouve les cookies. Ils se définissent comme « *des petits fichiers informatiques en format texte, qui contiennent des fragments d'informations, sont générés par un site Internet et sont placés dans le terminal*⁶⁴ de celui ou celle qui visite le site en question »⁶⁵. Selon le

⁵⁹ COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES (CNIL), *La publicité ciblée en ligne, communication présentée en séance plénière*, op. cit., p. 8.

⁶⁰ S. RANSE, « Le *profiling* des internautes au regard du droit au respect de la vie privée : le coût de l'efficacité ! », *R.D.T.I.*, n° 20/2004, p. 39.

⁶¹ *Ibid.*

⁶² Ces renseignements sont repris dans la section « *À propos* », présente sur le profil Facebook de chacun de ses utilisateurs, libre à eux de compléter plus ou moins assidument les différentes informations.

⁶³ J.-P. WALTER, *Le profilage des individus à l'heure du cyberspace : un défi pour le respect du droit à la protection des données*, op. cit., p. 4.

⁶⁴ Il peut s'agir d'un ordinateur, d'un Smartphone, d'une tablette, d'une console de jeux, etc.

⁶⁵ A. PHILIPPART DE FOY et K. VAN GOSSUM, « Les cookies : état des lieux et perspectives », *R.D.T.I.*, n° 52/2013, p. 6.

Groupe de travail « Article 29 »⁶⁶ (ci-après « G29 »), les cookies peuvent poursuivre divers objectifs, tels que mémoriser les préférences de l'internaute afin de pouvoir personnaliser sa navigation, ou encore recueillir des informations relatives à son utilisation lorsqu'il surfe sur des sites Web⁶⁷. Il faut dès lors s'entendre sur le fait que les cookies ne sont pas des logiciels et ne doivent pas être confondus avec des virus ou des *spywares*, puisqu'ils n'ont pas la capacité d'analyser le contenu du disque dur d'un ordinateur⁶⁸.

Les *spywares*, ou logiciels espions, sont quant à eux des programmes encore plus intrusifs, qui ont vocation à collecter et ensuite transmettre des informations (telles que le parcours de l'internaute sur le Web et l'adresse IP) à des sociétés de marketing⁶⁹. Le plus souvent cachés dans des logiciels gratuits, les effets des *spywares* peuvent varier : repérer les pages visitées par l'internaute, cibler les bannières publicitaires, rassembler les mots-clés des moteurs de recherche, récupérer les informations dévoilées lors d'une transaction en ligne, ou encore analyser les documents stockés sur l'ordinateur « *espionné* »⁷⁰. De précieux renseignements sont ainsi récoltés à l'insu du consommateur, qui n'a pas consenti à être « *pisté* » de la sorte et à recevoir de telles publicités personnalisées, basées sur son comportement⁷¹.

Section 2. L'analyse des données, ou « *data mining* »

Le *data mining* (littéralement : « *forage de données* ») peut se définir comme « *l'application des techniques de 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* ».

⁶⁶ Le Groupe de travail « Article 29 » est un organe consultatif européen indépendant sur la protection des données et de la vie privée, mis en place en vertu de l'article 29 de la directive 95/46/CE (qui était l'ancêtre du RGPD).

⁶⁷ A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 293.

⁶⁸ K. VAN GOSSUM, *Het Internet en de verwerking van persoonsgegevens door lokale besturen: algemeen overzicht en praktische toepassingen*, Brugge, Vanden Broele, 2012, p. 68 et G. SOMERS, « Can Confidentiality be upheld in the Information Society? », *R.E.D.C.*, 2011/3, p. 531.

⁶⁹ S. RANSE, « Le *profiling* des internautes au regard du droit au respect de la vie privée : le coût de l'efficacité ! », *op. cit.*, pp. 40-41.

⁷⁰ A. METOU, « Vous avez dit “spyware” ? », in *Technologies Internationales*, n° 86, juillet-août 2002, p. 34.

⁷¹ S. RANSE, « Le *profiling* des internautes au regard du droit au respect de la vie privée : le coût de l'efficacité ! », *op. cit.*, p. 41.

informatiques, en vue d'extraire des informations nouvelles et utiles pour le détenteur de ces données »⁷².

En pratique, les données préalablement collectées sont traitées par des programmes de calcul, de comparaison et de corrélation statistique, lesquels fonctionnent à l'aide d'algorithmes qui permettent notamment d'ordonner, de filtrer ou de regrouper les données par affinités⁷³. Il faut tout de même garder à l'esprit qu'étant donné le fait que les algorithmes utilisent des techniques basées sur les probabilités, il subsistera toujours « *un degré d'incertitude quant aux relations ou aux classifications qui en découlent* »⁷⁴.

Cette seconde étape vise à catégoriser les individus par rapport à leurs caractéristiques personnelles, qu'elles soient « *immuables* » (telles que l'âge ou la taille) ou « *modifiables* » (telles que les habitudes, les préférences ou d'autres éléments comportementaux)⁷⁵. Le *data mining* permet ainsi, sur base de certaines caractéristiques observables chez les individus, d'en déduire d'autres qui ne le sont pas, avec une certaine marge d'erreur⁷⁶. En d'autres termes, l'intérêt de cet outil informatique réside dans le fait qu'il est capable de « *faire parler* »⁷⁷ les données précédemment récoltées, afin de pouvoir dégager des profils⁷⁸.

En tant qu'instrument prédictif, il se montre d'une aide précieuse en matière de marketing et de gestion de clientèle, notamment en termes de personnalisation des pages du site Web de l'entreprise en fonction du profil de chaque internaute, et en termes d'identification de clients potentiels⁷⁹. Ainsi, l'entreprise « *se rapproche du consommateur, a des informations qui sont beaucoup plus performantes sur lui et un retour de sa part qui est également plus engageant* »⁸⁰.

⁷² S. TUFFERY, *Data mining et statistique décisionnelle. L'intelligence dans les bases de données*, Paris, Éd. Technip, 2005, p. VII.

⁷³ A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 292.

⁷⁴ AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE, *Guide pour la prévention du profilage illicite aujourd'hui et demain*, *op. cit.*, p. 23.

⁷⁵ *Ibid.*, pp. 17-18.

⁷⁶ J.-M. DINANT, C. LAZARO, Y. POULLET, N. LEFEVER et A. ROUVROY, *Application of Convention 108 to the profiling mechanism: Some ideas for the future work of the consultative committee (T-PD)*, Doc. T-PD 01, p. 3

⁷⁷ *Ibid.*, p. 9

⁷⁸ A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 292.

⁷⁹ J.-M. DINANT, C. LAZARO, Y. POULLET, N. LEFEVER et A. ROUVROY, *Application of Convention 108 to the profiling mechanism: Some ideas for the future work of the consultative committee (T-PD)*, *op. cit.*, pp. 10-11.

⁸⁰ Voy. en ce sens F. MEURICE, Head of Digital Service Design, interview réalisée par M.-E. RODRIGUEZ le 30 juillet 2020, p. 90

Section 3. L'application des données à un profil, ou « inférence »

La troisième et dernière étape n'est autre que l'application du profil de groupe à l'internaute en question, à partir de ses données personnelles préalablement collectées et analysées, et ce, dans le but de lui attribuer des données nouvelles qui font partie de la catégorie à laquelle il appartient⁸¹.

Le profil peut ainsi être défini comme « *un ensemble de données qui caractérise une catégorie d'individus et qui est destiné à être appliqué à un individu* »⁸². La Commission Nationale de l'Informatique et des Libertés (CNIL) distingue deux types de profil : un profil explicite qui est constitué à partir des données personnelles que l'internaute a lui-même fournies⁸³, et un profil prédictif qui se déduit de l'observation du comportement de l'internaute dans le temps ainsi que de ses différents clics (suivi des pages visitées, des mots-clés employés, des publicités qui ont attiré son attention, etc.)⁸⁴. Il est évident que ces deux approches peuvent être combinées⁸⁵.

On devine d'ores et déjà le danger encouru⁸⁶ : l'individu pourrait se voir réduit à un profil (qui pourrait au demeurant s'avérer incomplet ou inexact) construit sur base de méthodes automatiques, lesquelles sont susceptibles de servir de fondement à la prise de décision⁸⁷.

⁸¹ A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 292.

⁸² Recommandation CM/Rec(2010)13 du Comité des ministres aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, adoptée par le Comité des ministres le 23 novembre 2010.

⁸³ Notamment lorsque l'individu s'inscrit à un service en ligne ou qu'il divulgue certaines informations sur un réseau social.

⁸⁴ J.-P. WALTER, *Le profilage des individus à l'heure du cyberspace : un défi pour le respect du droit à la protection des données*, *op. cit.*, p. 9.

⁸⁵ COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES (CNIL), *La publicité ciblée en ligne*, *op. cit.*, p. 11.

⁸⁶ Nous reviendrons plus en détails sur les différents risques du profilage dans le cadre du Chapitre 3.

⁸⁷ J.-P. WALTER, *Le profilage des individus à l'heure du cyberspace : un défi pour le respect du droit à la protection des données*, *op. cit.*, p. 9.

Section 4. Le profilage aux fins de publicité ciblée en ligne constitue-t-il un traitement de données à caractère personnel ?

Tel que nous l'avons analysé, les différentes étapes du profilage ne portent pas toutes sur le traitement de données qui revêtent le caractère de données *personnelles*. Tout l'enjeu de cette qualification réside dans l'éventuelle application de la législation sur la protection des données à caractère personnel⁸⁸.

Autrefois sujet à controverse, le G29 a néanmoins su aplanir le débat, en ce qu'il estime que toutes les étapes relatives au profilage, de la collecte des données à la création du profil et à son application à l'internaute, doivent tomber dans le giron de la protection des données à caractère personnel⁸⁹.

En effet, tout le raisonnement se fonde sur la définition très large de données à caractère personnel, laquelle englobe « *toute information concernant une personne identifiée ou identifiable* »⁹⁰. Ainsi, bien que certains professionnels du profilage essaient encore de se cacher derrière l'anonymisation ou la pseudonymisation des données traitées⁹¹ afin d'échapper à la qualification de données personnelles⁹², il ne fait plus aucun doute que la législation sur la protection des données a vocation à s'appliquer « *dès que la publicité ciblée repose sur des goûts ou des comportements qui peuvent être rattachés à un individu identifié ou identifiable* »⁹³.

⁸⁸ A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 294.

⁸⁹ *Ibid.*, pp. 294-295.

⁹⁰ Voy. en ce sens GROUPE DE TRAVAIL « ARTICLE 29 », Avis 4/2007 sur le concept de données à caractère personnel, WP 136, (01248/07/FR), 20 juin 2007, pp. 6-13.

⁹¹ Sur les notions d'anonymisation et de pseudonymisation, voy. le Titre 3, Chapitre 1, Section 1.

⁹² A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 295.

⁹³ *Ibid.*, p. 298.

Chapitre 3. Les principaux risques du profilage

Malgré les avantages qu'il procure aux internautes, à l'économie et à la société de manière générale, le profilage engendre son lot de conséquences négatives sur le respect des droits et des libertés fondamentales, notamment le droit à la vie privée et à la protection des données⁹⁴.

Les pratiques de profilage peuvent exposer les individus à de graves menaces en termes de discrimination, d'exclusions et de restrictions de libertés, et particulièrement porter atteinte à leurs droits personnels et à leur dignité⁹⁵. Elles peuvent avoir pour conséquence d'empêcher, de manière injustifiée, l'accès à certains biens ou services : une personne pourrait être confrontée au refus de l'octroi d'un prêt à la suite d'une estimation de sa solvabilité ou d'une prédiction de son état de santé⁹⁶, tandis qu'une autre pourrait se voir refuser un emploi en raison de son orientation sexuelle, de ses opinions politiques, de sa race, ou même d'une erreur de jeunesse que le Web n'a pas oubliée⁹⁷.

Néanmoins, nous concentrerons essentiellement notre attention sur une autre problématique majeure du profilage sur Internet, à savoir le manque de transparence des traitements de données⁹⁸. Dans un monde interconnecté où les services sont pour la plupart gratuits, les internautes pensent naïvement surfer sur la toile en toute liberté, car ils n'aperçoivent pas de conséquence néfaste immédiate⁹⁹. Ainsi, ils exposent de manière désinhibée « *leur vie privée, leurs préférences, leurs modes de consommation, leurs activités et même leurs petits vices* »¹⁰⁰.

⁹⁴ J.-P. WALTER, *Le profilage des individus à l'heure du cyberspace : un défi pour le respect du droit à la protection des données*, op. cit., p. 2.

⁹⁵ A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », op. cit., pp. 280-281.

⁹⁶ J.-P. WALTER, *Le profilage des individus à l'heure du cyberspace : un défi pour le respect du droit à la protection des données*, op. cit., p. 7.

⁹⁷ A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », op. cit., p. 280.

⁹⁸ J.-P. WALTER, *Le profilage des individus à l'heure du cyberspace : un défi pour le respect du droit à la protection des données*, op. cit., p. 7.

⁹⁹ A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », op. cit., p. 277.

¹⁰⁰ *Ibid.*, p. 278.

Le profilage se déroule le plus souvent à l'insu de la personne concernée, qui se retrouve alors poussée à prendre des décisions ou à avoir certains comportements en ignorant complètement ce que détient le responsable de traitement à son sujet¹⁰¹. En définitive, l'individu numérisé n'est pas le résultat d'une construction d'identité autonome, mais découle – au moins partiellement – des algorithmes de classification qui servent à créer des profils¹⁰².

Le processus du profilage donne par conséquent naissance à une réalité construite de toutes pièces qui peut entraîner une manipulation¹⁰³ des consommateurs, en mettant à mal leur libre-arbitre, en diminuant leur pouvoir décisionnel, voire même en devançant leurs envies au moment où ils se montrent le plus vulnérables¹⁰⁴. Ces derniers ne distinguent finalement plus s'ils posent leurs choix par eux-mêmes ou en fonction des profils qui leur sont appliqués¹⁰⁵. On peut parler d'une certaine « *érosion de la capacité des consommateurs à participer au processus décisionnel les concernant* »¹⁰⁶, voire même du danger d'en arriver à une « *acceptation quasi-automatique de la validité et de la pertinence de ces décisions* »¹⁰⁷. À terme, la confiance que les utilisateurs éprouvent pour les services numériques pourraient véritablement se détériorer¹⁰⁸.

¹⁰¹ J.-P. WALTER, *Le profilage des individus à l'heure du cyberspace : un défi pour le respect du droit à la protection des données*, op. cit., p. 8.

¹⁰² Ibid., p. 6.

¹⁰³ COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, Avis 29/2007 relatif aux nouveaux modes de consommation médiatique et à la protection de la vie privée, 19 septembre 2007, p. 6, point 32 : « *Toute utilisation des services de médias, et notamment de leurs possibilités d'interactivité, dans le but d'influencer le comportement des utilisateurs pourrait constituer une atteinte à la dignité de ces derniers, à leur intégrité et à leurs droits fondamentaux. Elle doit donc être proscrite* ».

¹⁰⁴ A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », op. cit., p. 280.

¹⁰⁵ V. FOSSOUL, « L'identification par radiofréquence (RFID) : reflet des nouvelles tendances en matière de protection des données à caractère personnel », op. cit., p. 128.

¹⁰⁶ Ibid. Voy. également les extraits des travaux préparatoires cités par L. A. BYGRAVE : « *The use of extensive data profiles of individuals by powerful public and private institution deprives the individual the capacity to influence decision-making processes within those institutions, should decisions be taken on the sole basis of his 'data shadow'* » L. A. BYGRAVE, *Minding the machine: article 15 of the EC Data Protection Directive and Automated Profiling* (disponible sur <http://classic.austlii.edu.au/au/journals/PrivLawPRpr/2000/40.html>, page consultée le 5 mai 2020).

¹⁰⁷ J.-M. DINANT, C. LAZARO, Y. POULLET, N. LEFEVER et A. ROUVROY, *L'application de la Convention 108 au mécanisme de profilage : Éléments de réflexion destinés au travail du futur Comité consultatif (T-PD)*, op. cit., p. 14. Dans le même ordre d'idée, comme le souligne V. DEGREEF : « *L'individu en arrive à ne pas savoir si les décisions qu'il prend sont le fruit de sa personne – même si cette personne se construit en rapport avec les autres – ou simplement le fruit des profils qui lui sont appliqués* » V. DEGREEF, *La maîtrise du soi multiple face à l'exhibitionnisme identitaire. L'identité en termes de contrôle et d'autonomie au travers des logiciels sociaux*, Série des Working Papers du Centre Perelman de philosophie du droit n° 2008/4, Année académique 2007-2008, (disponible sur <https://www.philodroit.be/La-maitrise-du-soi-multiple-face-a?lang=fr>, page consultée le 20 avril 2020).

¹⁰⁸ A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », op. cit., p. 278.

Enfin, il ne faut pas oublier que le profilage n'est pas une science exacte. Les erreurs commises par le processus pourraient ainsi précipiter la prise de mauvaises décisions, à cause de données mal collectées ou mal interprétées. Dès lors, il est primordial de ne pas « *réduire un individu à un profil généré de façon automatisée* »¹⁰⁹ en faisant complètement abstraction de sa force de résilience et de sa volonté. Il est donc indispensable d'offrir à la personne la garantie suffisante de pouvoir « *lutter contre son profil* »¹¹⁰.

¹⁰⁹ A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 280.

¹¹⁰ V. FOSSOUL, « L'identification par radiofréquence (RFID) : reflet des nouvelles tendances en matière de protection des données à caractère personnel », *op. cit.*, p. 128.

Titre 2. La publicité ciblée opérée par Facebook

Une pluralité de sources du droit a vocation à s'appliquer à une plateforme comme Facebook¹¹¹ : le droit des contrats installe le cadre juridique de base sur lequel est construit le réseau social ; le droit des pratiques du marché et de la protection des consommateurs (notamment consacré dans la loi sur les pratiques du marché¹¹²) doit évidemment être évoqué ; le droit international privé est également fortement sollicité – étant donné que Facebook est un réseau social sans frontière – afin d'identifier le juge et les textes de lois applicables pour trancher le litige ; *last but not least*, le RGPD, autrefois directive 95/46¹¹³, transposée dans la loi vie privée¹¹⁴, elle-même révisée¹¹⁵.

Ainsi, le respect des dispositions légales ou réglementaires doit être observé tant en amont, pour le traitement des données à caractère personnel¹¹⁶, qu'en aval, pour le lancement d'une campagne publicitaire ciblée¹¹⁷. Toutefois, par soucis de cohérence et parce que nous ne pouvons pas nous permettre d'être exhaustifs en une soixantaine de pages, nous nous concentrerons uniquement sur les exigences imposées par le RGPD, qui s'avèrent particulièrement sollicitées dans le contexte des réseaux sociaux.

¹¹¹ J.-P. MOINY et Y. POULLET, « Les réseaux sociaux, le droit et les volontés qui les animent », in *Social Media : le droit ou l'anarchie ? / Social Media : recht of anarchie*, Bruxelles, Bruylant, 2012, pp. 7-9.

¹¹² L'ancienne Loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur, *M.B.*, 29 août 1991, est aujourd'hui remplacée par la Loi du 6 avril 2010 relative aux pratiques du marché et à la protection du consommateur, *M.B.*, 12 avril 2010, p. 2084.

¹¹³ Directive (CE) n° 95/46 du Parlement 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, 23 novembre 1995 (abrogée).

¹¹⁴ Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, p. 5801.

¹¹⁵ Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, p. 68616.

¹¹⁶ Le « traitement de données » couvre toute opération effectuée sur des données à caractère personnel, comme nous le verrons plus en détails dans le Chapitre 1, Section 2, § 1^{er} sur le Champ d'application matériel. Voy. en ce sens AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, *op. cit.*, p. 110.

¹¹⁷ H. JACQUEMIN, « Le big data à l'épreuve des pratiques du marché et de la protection du consommateur », *R.D.T.I.*, n° 70/2018, p. 79.

Chapitre 1. L'applicabilité du RGPD à Facebook

Même s'il n'existe aucun doute quant au fait que l'apparition du RGPD sur la scène législative européenne représente une avancée significative et symbolique en termes de protection des données à caractère personnel, il semble toutefois nécessaire de s'assurer de l'impact que peut réellement avoir une telle réglementation sur un géant d'Internet comme Facebook. Partant, dans la première Section, nous commencerons par définir brièvement ce qu'est Facebook, ainsi que la mission que poursuit le RGPD. Ensuite, dans la deuxième Section, nous délimiterons le champ d'application du règlement, et la manière dont la théorie se transpose à la réalité du cas Facebook.

Section 1. Considérations préliminaires

§1. Quelques notions élémentaires à propos de Facebook

L'internaute peut être amené à jouer un rôle d'une importance considérable en ce qui concerne la transmission de ses propres données, notamment lorsqu'il navigue sur les réseaux sociaux¹¹⁸.

Facebook « *can be defined as [a] website whose main purpose is to act as a connector among users* »¹¹⁹. La plateforme offre dès lors aux utilisateurs la possibilité d'entrer en interactivité les uns avec les autres, et permet de construire des relations sociales entre des individus qui partagent les mêmes centres d'intérêts¹²⁰. Pour avoir accès au service qu'il propose, le site Web requiert des internautes qu'ils mettent à disposition un certain nombre de données personnelles, aux fins de créer un « *profil* »¹²¹.

Le réseau social est ainsi responsable de la gestion des profils, ainsi que du contenu déposé par les membres. Il s'agit là de sa première activité : le stockage d'une quantité inimaginable d'informations, et la mise à disposition de celles-ci aux autres utilisateurs du

¹¹⁸ A. ARAMAZANI, « Le droit à l'oubli et internet », *R.D.T.I.*, 2011/2, n° 43, p. 44.

¹¹⁹ A. LEVIN et P. SANCHEZ ABRIL, "Two Notions of Privacy Online", in *Vanderbilt J. of Ent. And Tech. Law*, 2009, p. 1017.

¹²⁰ GROUPE DE TRAVAIL « ARTICLE 29 », Avis 5/2009 sur les réseaux sociaux en ligne, WP 163, 12 juin 2009, (01189/09/FR), p. 4.

¹²¹ A. ARAMAZANI, « Le droit à l'oubli et internet », *op. cit.*, p. 44.

réseau, selon une réglementation définie en partie par les usagers mais également et surtout par le réseau social lui-même, au moyen de paramètres de confidentialité plus ou moins modulables¹²².

Mais ce n'est pas tout, les entreprises sont également présentes et actives sur les plateformes telles que Facebook, grâce auxquelles elles disposent d'une vitrine facilement accessible et performante afin de diffuser des annonces publicitaires de plus en plus ciblées¹²³. Grâce aux nombreuses informations publiées sur leurs profils, les utilisateurs, le plus souvent de manière inconsciente, offrent ainsi de précieux renseignements aux publicitaires¹²⁴.

§2. Le rôle du RGPD dans le paysage législatif

Le RGPD, réforme ambitieuse du droit de la protection des données à caractère personnel¹²⁵, vise avant tout l'harmonisation de vingt-huit pratiques différentes au sein de l'Union européenne¹²⁶, de façon à ce que la protection offerte soit comparable, mais surtout que les frontières floues de la vie privée soient entendues et appréhendées de façon uniforme partout sur le continent européen¹²⁷. Ainsi, même si les États ont bénéficié d'une certaine marge de manœuvre pour transposer le RGPD dans leurs lois nationales, la finalité poursuivie restait bel et bien d'atteindre un certain degré d'uniformisation¹²⁸.

En outre, même s'il est vrai qu'il a fait peser de plus lourdes responsabilités sur le dos des entreprises et des autorités publiques¹²⁹, il faut garder à l'esprit que l'objectif de départ du

¹²² J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *R.E.D.C.*, 2010/2, pp. 236-243.

¹²³ M. SALMON et J. DESCHUYTENEER, « Introduction », in *Les réseaux sociaux et le droit*, Bruxelles, Éditions Larcier, 2014, p. 8.

¹²⁴ A. ARAMAZANI, « Le droit à l'oubli et internet », *op. cit.*, p. 44.

¹²⁵ E. CRUYSMANS, « La directive 95/46/CE n'est plus, vive le R.G.P.D. ! », in *Auteurs & Media*, Vol. 2017, no. 1, p. 108.

¹²⁶ P. DE BACKER, « Préface », in *Data protection & privacy : le GDPR dans la pratique*, Limal, Anthemis, 2017, p. 11.

¹²⁷ N. RAGHENO, « Droits fondamentaux et société numérique : la vie privée existe-t-elle encore ? », in *Data protection & privacy : le GDPR dans la pratique*, Limal, Anthemis, 2017, p. 19.

¹²⁸ C. PONSART ET R. ROBERT, « Le règlement européen de protection des données personnelles », *J.T.*, 2018, p. 422.

¹²⁹ N. RAGHENO ET P. LAMBRECHT, « Avant-propos », in *Data protection & privacy : le GDPR dans la pratique*, Limal, Anthemis, 2017, p. 15.

RGPD était de favoriser le bon développement du marché numérique européen¹³⁰, en assurant la libre circulation des données et des services numériques¹³¹.

Enfin, le RGPD avait également pour vocation de s'adapter aux nouvelles technologies¹³², sans quoi l'importante remise à niveau des normes en matière de protection des données n'aurait pas été possible¹³³. Cet instrument européen a ainsi permis d'« *assurer tout leur effet utile aux règles de protection des données dans le contexte d'une industrie numérique mondialisée* »¹³⁴.

Section 2. Champ d'application

Bien que les champs d'application matériel, personnel et territorial du RGPD soient généralement présentés de manière distincte dans un souci de clarté, on ne peut nier que les trois facettes sont en réalité – pour reprendre un des termes fétiches de la Cour de justice de l'Union européenne (ci-après « CJUE ») en matière de protection des données – « *inextricablement* » liées, et doivent dès lors être appréhendées ensemble¹³⁵.

§1. Champ d'application matériel

L'article 3 du RGPD¹³⁶ prévoit que le règlement « *s'applique au traitement de données à caractère personnel* ». Encore reste-il à déterminer ce que recouvrent les notions de traitement (A) et de données à caractère personnel (B).

¹³⁰ P. DE BACKER, « Préface », *op. cit.*, p. 11.

¹³¹ 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 LEGER L.), janvier 2018 (disponible sur <https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf>, page consultée le 06 août 2020), p. 77.

¹³² N. RAGHENO, « Droits fondamentaux et société numérique : la vie privée existe-t-elle encore ? », *op. cit.*, p. 19.

¹³³ A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *R.D.T.I.*, 2018/1, n° 70, p. 20.

¹³⁴ 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'Internet*, Bruxelles, Bruylant, 2019, p. 476.

¹³⁵ S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, Bruxelles, Bruylant, 2005, p. 8.

¹³⁶ En ce qui concerne le champ d'application matériel, nous nous concentrerons uniquement sur les notions présentes dans l'art. 3 du RDPG (nous n'examinerons pas l'ensemble des notions de l'art. 2).

A. Un « traitement »

Selon le RGPD, le traitement se définit 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* »¹³⁷. Les procédés automatisés regroupent toutes les « *technologies informatiques permettant de traiter des données, actuelles ou à venir* »¹³⁸. En réalité, la définition du traitement couvre donc une très grande variété d'opérations, à tel point qu'en règle générale, dès qu'il est question de données personnelles, il est très probablement également question de traitement au sens du RGPD¹³⁹.

B. De « données à caractère personnel »

La notion de « *données à caractère personnel* » a également tendance à élargir l'ensemble des hypothèses couvertes par le RGPD, puisque celle-ci vise « toute information se rapportant à une personne physique identifiée ou identifiable »¹⁴⁰. Déjà sous l'ère de la directive n° 95/46, la volonté du législateur européen était d'adopter la définition « *la plus globale possible de la notion de données à caractère personnel, afin de couvrir toutes les informations qui peuvent être reliées à une personne* »¹⁴¹. Le G29 – remplacé aujourd'hui par le Comité européen de la protection des données¹⁴² – ainsi que la CJUE¹⁴³ ont confirmé la nature extrêmement large du concept¹⁴⁴.

Il est possible de décortiquer la définition en trois temps. Premièrement, le RGPD a vocation à s'appliquer à toute information, « *quel que soit son format, son origine ou son*

¹³⁷ RGPD, art. 4, b).

¹³⁸ A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, p. 16.

¹³⁹ F. BORGESIU, "Singling out people without knowing their names: behavioural targeting, pseudonymous data, and the new Data Protection Regulation", in *Computer Law & Security Review*, 2016, p. 259.

¹⁴⁰ Souligné par nos soins. Voy. en ce sens RGPD, art. 4, 1).

¹⁴¹ Voy. la Proposition amendée de directive du Conseil et du Parlement européen sur la protection des individus au regard du traitement de leurs données à caractère personnel, 15 octobre 1992, COM (92)422 final, p. 10.

¹⁴² RGPD, art. 68 et suivants.

¹⁴³ C.J.U.E., arrêt *Göta hovrätt contre Lindqvist*, 6 novembre 2003, C-101/01, EU:C:2003:596, pts. 24-27 ; C.J.U.E., arrêt *Rechnungshof contre Österreichischer Rundfunk et autres*, 20 mai 2003, C-465/00, EU:C:2003:294, pt. 64 ; C.J.U.E., arrêt *Tietosuojavaltuutettu contre Satakunnan Markkinapörssi Oy et Satamedia*, 16 décembre 2008, C-73/07, EU:C:2008:727, pts. 35-37 ; C.J.U.E., arrêt *Republik Österreich contre Martin Huber*, 16 décembre 2008, C-524/06, EU:C:2008:724, pt. 43 ; C.J.U.E., arrêt *College van burgemeester en wethouders van Rotterdam contre M.E.E. Rijkeboer*, 7 mai 2009, C-553/07, EU:C:2009:293, pt. 62 ; C.J.U.E., arrêt *Bonnier Audio AB e.a. contre Perfect Communication Sweden AB*, 19 avril 2012, C-461/10, EU:C:2009:293, pt. 93.

¹⁴⁴ GROUPE DE TRAVAIL « ARTICLE 29 », Avis 4/2007 sur le concept de données à caractère personnel, *op. cit.*, pp. 6-13.

support »¹⁴⁵, sans importance quant au fait qu'elle soit « *exacte ou inexacte, objective ou subjective* »¹⁴⁶, et ne se limitant pas aux seules informations relatives à la vie privée et familiale¹⁴⁷, mais s'étendant au contraire à « *l'ensemble des informations se rapportant à la personne concernée, en ce compris les informations qui sont publiques* »¹⁴⁸. Deuxièmement, même si le RGPD est de nature à s'appliquer à tout type d'information, il ne compte s'appliquer qu'aux informations se rapportant à une personne identifiée ou identifiable. Selon la CJUE¹⁴⁹, « *il faut, ou plutôt il suffit, que l'information soit liée à une personne déterminée en raison de son contenu, de sa finalité ou de son effet* »¹⁵⁰. Troisièmement, le dernier élément de la définition repose sur la vérification que l'information se rapporte bien à une personne physique identifiée ou identifiable, ce qui ne peut être le cas que si des identifiants existent, c'est-à-dire « *des informations spécifiques qui présentent une relation particulièrement privilégiée et étroite avec la personne physique concernée* »¹⁵¹.

Aux termes de ces considérations, il ne fait donc aucun doute que le domaine d'activités de Facebook entre dans le champ d'application matériel du RGPD : la plateforme opère bel et bien des traitements (lesquels sont toujours considérés comme automatisés)¹⁵² qui ont trait aux données des utilisateurs, aisément identifiables grâce à leur profil personnalisé.

§2. Champ d'application personnel

Pour savoir si une hypothèse entre dans le champ d'application de l'article 3 du RGPD, il est nécessaire d'identifier le ou les responsables du traitement (A) et, le cas échéant,

¹⁴⁵ GROUPE « ARTICLE 29 », Avis 4/2007 sur le concept de données à caractère personnel, *op. cit.*, pp. 6-9. Voy. également L. COUDRAY, *La protection des données personnelles dans l'Union européenne : naissance et consécration d'un droit fondamental*, Sarrebruck, Éditions Universitaires Européennes, 2010, pp. 118-121.

¹⁴⁶ C.J.U.E., arrêt *Peter Nowak contre Data Protection Commissioner*, 20 décembre 2017, C-434/16, EU:C:2017:994, pt. 34 ; GROUPE « ARTICLE 29 », Avis 4/2007 sur le concept de données à caractère personnel, *op. cit.*, pp. 6-9 ; L. COUDRAY, *La protection des données personnelles dans l'Union européenne : naissance et consécration d'un droit fondamental*, *op. cit.*, pp. 118-121.

¹⁴⁷ *Ibid.*

¹⁴⁸ 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. 56.

¹⁴⁹ C.J.U.E., arrêt *Peter Nowak contre Data Protection Commissioner*, *op. cit.*

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. 56.

¹⁵¹ GROUPE DE TRAVAIL « ARTICLE 29 », Avis 4/2007 sur le concept de données à caractère personnel, *op. cit.*, p. 13.

¹⁵² J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, pp. 242-243.

l'hypothèse de la responsabilité conjointe (B) ou encore, le ou les sous-traitants qui prennent part au traitement des données à caractère personnel (C).

A. Le responsable de traitement

Le règlement définit le responsable du traitement 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* »¹⁵³. Le G29 utilise d'ailleurs l'expression de « *maître du fichier* »¹⁵⁴.

Pour être qualifié de responsable du traitement, l'opérateur doit être en mesure d'exercer une influence sur les décisions ayant trait aux finalités et aux moyens du traitement¹⁵⁵. Élevée au rang d'élément décisif en termes de qualification, cette influence « *peut découler directement ou indirectement de la loi* »¹⁵⁶, même si, en règle générale, il s'agira d'une influence de fait, qui s'accompagnera d'une appréciation factuelle¹⁵⁷. En fait, le seuil minimal d'influence requis par l'entité en question n'est autre que de disposer d'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* »¹⁵⁸.

Partant, la plateforme Facebook peut être qualifiée de responsable de traitement des données qu'elle collecte, étant donné que c'est à elle que revient la décision du « *comment* » et du « *pourquoi* »¹⁵⁹ les données seront traitées¹⁶⁰. En ce sens, le G29 considère d'ailleurs généralement les fournisseurs de réseaux sociaux comme des responsables de traitement¹⁶¹.

¹⁵³ RGPD, art. 4, 7).

¹⁵⁴ GROUPE DE TRAVAIL « ARTICLE 29 », Avis 1/2010 sur les notions de responsable du traitement et de sous-traitant, WP 169, 16 février 2010, (00264/10/FR), p. 4.

¹⁵⁵ 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.

¹⁵⁶ *Ibid.*

¹⁵⁷ *Ibid.*

¹⁵⁸ GROUPE DE TRAVAIL « ARTICLE 29 », Avis 1/2010 sur les notions de responsable du traitement et de sous-traitant, *op. cit.*, p. 14.

¹⁵⁹ 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.

¹⁶⁰ J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, pp. 254-255.

¹⁶¹ GROUPE DE TRAVAIL « ARTICLE 29 », Avis 5/2009 sur les réseaux sociaux en ligne, *op. cit.*, p. 5.

B. L'hypothèse de la responsabilité conjointe

L'article 26 du RGPD définit les responsables conjoints comme « *deux responsables du traitement ou plus qui déterminent conjointement les finalités et les moyens du traitement* ». Dans une telle hypothèse, les responsables conjoints doivent « *par voie d'accord entre eux* »¹⁶² définir de manière transparente et claire leurs obligations respectives¹⁶³.

À titre d'illustration, dans l'arrêt *Fanpage*¹⁶⁴, la CJUE considère que le statut d'administrateur d'une page « *fan* » sur le réseau social Facebook entraîne, au même titre que la société Facebook elle-même et conjointement avec celle-ci, la qualification de « *responsable du traitement* »¹⁶⁵. En effet, la CJUE est d'avis que l'administrateur s'implique dans la détermination des finalités et des moyens, et qu'il exerce dès lors une influence sur ce processus, notamment parce que par le biais de la création de sa page, il « *offre à Facebook la possibilité de placer des cookies sur l'ordinateur ou sur tout autre appareil* »¹⁶⁶ de l'internaute qui visite sa page « *fan* », ce qui lui permet en définitive de « *définir, au travers des filtres mis à sa disposition par Facebook, les critères à partir desquels les statistiques des visites de sa page 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* »¹⁶⁷.

Toutefois, qui dit responsabilité conjointe, ne dit pas forcément responsabilité équivalente¹⁶⁸. En pratique, il faut évaluer *in fine* la responsabilité respective des deux acteurs « *en tenant compte de toutes les circonstances pertinentes* »¹⁶⁹, même si la CJUE semble aller dans le sens d'une responsabilité plus lourde pour l'administrateur de la page « *fan* »¹⁷⁰.

¹⁶² Selon le GDPR, art. 26, § 1^{er}, la seule exception dans laquelle un tel accord n'est pas obligatoire est l'hypothèse où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'Etat membre auquel les responsables du traitement sont soumis.

¹⁶³ Voy. également le RGPD, considérant n° 79.

¹⁶⁴ C.J.U.E., arrêt *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein contre Wirtschaftsakademie Schleswig-Holstein GmbH*, 5 juin 2018, C-210/16, EU:C:2018:388 (ci-après l'arrêt « *Fanpage* »).

¹⁶⁵ E. CRUYSMANS, « Vous gérez une page « fan » sur Facebook ? Vous êtes alors coresponsable du traitement des données personnelles », in *Les pages : obligations, contrats et responsabilités*, Vol. 2018, no. 32, p. 1.

¹⁶⁶ C.J.U.E., arrêt *Fanpage*, *op. cit.*, pt. 35.

¹⁶⁷ 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.

¹⁶⁸ E. CRUYSMANS, « Vous gérez une page « fan » sur Facebook ? Vous êtes alors coresponsable du traitement des données personnelles », *op. cit.*, p. 1.

¹⁶⁹ C.J.U.E., arrêt *Fanpage*, *op. cit.*, § 43.

¹⁷⁰ *Ibid.*, § 41.

D'un côté, ce mode de raisonnement nous paraît assez logique et pertinent, étant donné que « *le fait pour un administrateur d'une page « fan » d'utiliser la plate-forme mise en place par Facebook, afin de bénéficier des services y afférents, ne saurait l'exonérer du respect de ses obligations* »¹⁷¹. D'un autre côté, il semble indispensable de nuancer nos propos, car pour de simples administrateurs de pages qui proposeraient des publicités ciblées, la société Facebook Ireland a décrété « *prendre la responsabilité principale en vertu du RGPD pour le traitement des données statistiques* »¹⁷² et souligne qu'elle seule est en position de « *prendre et mettre en œuvre des décisions concernant le traitement des données statistiques* »¹⁷³. Néanmoins, ce qui précède ne vaut que si l'accord correspond à la réalité des faits¹⁷⁴ : « *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* »¹⁷⁵.

C. Le sous-traitant, et sa relation avec le responsable de traitement

Le sous-traitant est défini par le règlement 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* »¹⁷⁶.

À l'instar des responsables conjoints qui doivent conclure un « *accord* », le responsable de traitement et le sous-traitant doivent conclure un « *contrat, ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre* »¹⁷⁷, qui va lier les deux acteurs mais également définir « *l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement* ».

S'il est vrai que Facebook fait appel à des sous-traitants, notamment en ce qui concerne ses algorithmes, il arrive que la société agisse également elle-même en qualité de

¹⁷¹ C.J.U.E., arrêt *Fanpage*, *op. cit.*, § 40.

¹⁷² Facebook, *Addenda concernant le responsable de traitement des données Statistiques* (disponible sur https://www.facebook.com/legal/terms/page_controller_addendum, page consultée le 10 juillet 2020).

¹⁷³ *Ibid.*

¹⁷⁴ RGPD, art. 26, § 2.

¹⁷⁵ A. DELFORGE, « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.*, p. 375.

¹⁷⁶ RGPD, art. 4, § 8.

¹⁷⁷ RGPD, art. 28, § 3.

sous-traitant. C'est par exemple le cas lorsque Facebook analyse les données récoltées sur son site Web pour en retirer des statistiques, qui seront utiles aux fins d'informer un annonceur sur l'efficacité de ses publicités ciblées¹⁷⁸.

Il est indéniable que dans ce genre de situation, Facebook agit pour le compte d'autrui. Toutefois, par ce biais, la plateforme n'agit-elle pas également pour servir ses propres intérêts, notamment afin d'augmenter le rendement des bannières publicitaires qu'elle propose ? Quoi qu'il en soit, il s'avère que le RGPD s'efforce d'assurer « *un resserrement des obligations* »¹⁷⁹ entre ces deux protagonistes, en mettant à charge de ces derniers le respect des exigences imposées par le règlement¹⁸⁰. Pour notre analyse, nous nous limiterons au fait que Facebook, comme il l'admet lui-même, agit dans la majorité des cas en tant que responsable de traitement¹⁸¹.

§3. *Champ d'application territorial*

Après avoir identifié le responsable du traitement ainsi que les éventuels responsables conjoints ou sous-traitants, il faut s'interroger sur la localisation de leurs établissements (A), et en fonction, déterminer l'application du RGPD dans le cas d'un établissement sur le territoire de l'Union (B), ainsi que dans le cas où ni le responsable, ni le sous-traitant, ne sont établis sur le territoire de l'Union (C).

A. La localisation de l'établissement

S'il est vrai que le texte du règlement ne définit pas ce qu'est à proprement parler un « *établissement* »¹⁸², un considérant vient préciser que le concept suppose avant tout « *l'exercice effectif et réel d'une activité au moyen d'un dispositif stable* »¹⁸³, sans importance quant à la forme juridique dudit dispositif¹⁸⁴. En ce sens, la CJUE a retenu une « *conception souple de la notion d'établissement, qui écarte toute approche formaliste selon laquelle une*

¹⁷⁸ Facebook Business, *Qu'est-ce que le Règlement général sur la protection des données (RGPD) ?* (disponible sur <https://www.facebook.com/business/gdpr>, page consultée le 12 juillet 2020).

¹⁷⁹ N. BINCTIN, « Partie 2 : Créer une patrimonialité des données à droit constant », *op. cit.*, p. 82.

¹⁸⁰ *Ibid.*

¹⁸¹ Facebook Business, *Qu'est-ce que le Règlement général sur la protection des données (RGPD) ?* (disponible sur <https://www.facebook.com/business/gdpr>, page consultée le 12 juillet 2020).

¹⁸² Par contre, l'« *établissement principal* » est défini dans le RGPD, art. 4, 16).

¹⁸³ RGPD, considérant n° 22.

¹⁸⁴ RGPD, considérant n° 22.

entreprise ne serait établie que dans le lieu où elle est enregistrée »¹⁸⁵ et souligne que « *cela vaut tout particulièrement pour des entreprises qui s'emploient à offrir des services exclusivement sur Internet* »¹⁸⁶.

En pratique, Facebook dispose de plusieurs bureaux dans divers pays européens, notamment à Dublin (d'ailleurs considéré comme le siège principal¹⁸⁷, surtout depuis que le réseau social a décidé de l'élever au rang d'« *International Headquarters* »¹⁸⁸), ce qui remplit sans l'ombre d'un doute les exigences légales et jurisprudentielles précitées.

Partant, deux précisions méritent d'être soulignées : premièrement, « *aucun lien de connexion entre la personne concernée et l'Union n'est requis pour l'application de ce point* »¹⁸⁹, ce qui implique qu'est visée « *toute personne* », sans distinction quant à sa nationalité ou son lieu de résidence¹⁹⁰, 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* »¹⁹¹; deuxièmement, le lieu où les données sont réellement traitées n'a pas d'importance¹⁹².

B. Le cas d'un établissement situé sur le territoire de l'Union

L'article 3, paragraphe 1^{er} du RGPD est rédigé comme suit : « *le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités*¹⁹³ *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* ».

Comme déjà décrit ci-dessus, la société Facebook dispose de plusieurs établissements en Europe, dont le plus important se situe à Dublin. Le point qui reste à éclaircir concerne la

¹⁸⁵ C.J.U.E., arrêt *Weltimmo s. r. o. contre Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1^{er} octobre 2015, C-230/14, EU:C:2015:639, pt. 29.

¹⁸⁶ *Ibid.*

¹⁸⁷ J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, p. 238.

¹⁸⁸ Facebook Newsroom, *Facebook to Establish International Headquarters in Dublin Ireland*, le 2 octobre 2008 (disponible sur <https://newsroom.fb.com/news/2008/10/facebook-to-establish-international-headquarters-in-dublin-ireland/>, page consultée le 15 juillet 2020).

¹⁸⁹ N. MICHAÏL, « 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.

¹⁹⁰ *Ibid.*

¹⁹¹ *Ibid.*

¹⁹² A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *op. cit.*, pp. 19-20.

¹⁹³ Souligné par nos soins.

question de savoir quels traitements sont exactement opérés « *dans le cadre des activités* » de l'établissement dublinois, pour déterminer quels traitements s'avèrent réellement soumis aux exigences imposées par le RGPD.

Les critères à l'aide desquels il est possible de déterminer si un traitement entre « *dans le cadre des activités* » d'un établissement sont les suivants¹⁹⁴ : dans un premier temps, il y a lieu d'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* »¹⁹⁵ ; dans un deuxième temps, il est question de vérifier s'il existe un « *lien indissociable* »¹⁹⁶ entre lesdites activités et le traitement.

À titre d'illustration, la CJUE a estimé, dans le cadre d'une affaire relative à Google et l'une de ses filiales, située en Espagne¹⁹⁷, que le lien entre le traitement des données opéré par Google et « *la promotion et la vente des espaces publicitaires* »¹⁹⁸ proposées par Google Spain était bel et bien établi, confirmation apportée par le fait que ces activités « *constituent le 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 activités* »¹⁹⁹.

Dès lors, ce raisonnement confirme, si besoin est, que la société Facebook Ireland, « *spécialisée dans le secteur d'activité du traitement de données, hébergement et activités connexes* »²⁰⁰, entre parfaitement dans le giron de cette première hypothèse, et est ainsi soumise aux prescrits légaux établis par le RGPD.

¹⁹⁴ N. MICHAÏL, « 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.

¹⁹⁵ GROUPE DE TRAVAIL « ARTICLE 29 », Avis 8/2010 sur le droit applicable, WP 179, 16 décembre 2010, (0836-02/10/FR), p. 2.

¹⁹⁶ WORKING PARTY « ARTICLE 29 », Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain, WP 179 update, 16 décembre 2015 (176/16/EN), p. 8.

¹⁹⁷ C.J.U.E., arrêt *Google Spain SL, Google Inc. contre Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, 13 mai 2014, C-131/12, EU:C:2014:317, pt. 60.

¹⁹⁸ *Ibid.*

¹⁹⁹ *Ibid.*, pt. 56.

²⁰⁰ X., *Fiche d'entreprise de Facebook Ireland* (disponible sur <https://www.societe.com/societe/facebook-ireland-limited-814665519.html>, page consultée le 15 juillet 2020).

C. Le cas d'un établissement situé en dehors du territoire de l'Union

Si l'on imaginait que les bureaux européens de Facebook n'existaient pas, il resterait tout de même un moyen de faire appliquer le RGPD au traitement de données en question : la seule condition requise serait alors que l'utilisateur concerné par ledit traitement se trouve sur le territoire de l'Union²⁰¹. Soupape de protection supplémentaire, la disposition a été envisagée dans le but « *d'éviter que le responsable du traitement puisse échapper à l'application du GDPR en contournant le paragraphe 1* »²⁰².

Par conséquent, les deux cas de figure dans lesquels le RGPD aura vocation à s'appliquer à une entreprise qui ne possède aucun établissement en Europe sont les suivants : lorsque les activités du traitement sont liées « *à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non des personnes* »²⁰³ ou « *au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union* »²⁰⁴. Une fois encore, il est incontestable que Facebook s'inscrit dans ces deux cas de figure : d'un côté, parce que Facebook offre un service gratuit à ses utilisateurs, et d'un autre côté, parce que Facebook opère un traçage des internautes, notamment à des fins de ciblage publicitaire, comme nous l'avons vu précédemment.

Chapitre 2. Les exigences imposées par le RGPD

Section 1. Les conditions de licéité du traitement

Conformément à l'article 6, paragraphe 1^{er} du RGPD, six bases juridiques peuvent justifier la licéité d'un traitement de données à caractère personnel, étant entendu que seul le respect de l'une d'entre elles est requis pour que le traitement soit considéré comme licite. Notre attention se portera sur le consentement²⁰⁵ et l'intérêt légitime²⁰⁶, fondements

²⁰¹ RGPD, art. 3, § 2.

²⁰² N. MICHAÏL, « 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.

²⁰³ RGPD, art. 3, § 2, a).

²⁰⁴ RGPD, art. 3, § 2, b).

²⁰⁵ RGPD, art. 6, § 1^{er}, a).

²⁰⁶ RGPD, art. 6, § 1^{er}, f).

juridiques privilégiés par Facebook lors du traitement de données personnelles à des fins de profilage publicitaire.

§1. Le consentement

L'article 4, paragraphe 11, du RGPD définit le consentement comme suit : « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* ». En outre, le G29 précise que « *les exigences relatives au consentement imposées par le RGPD ne sont pas considérées comme des « obligations supplémentaires », mais plutôt comme des conditions préalables essentielles au traitement licite* »²⁰⁷.

Premièrement, le consentement *libre* ne peut être valable que si l'individu concerné dispose d'une véritable liberté de choix²⁰⁸ et qu'il n'existe pas dans les faits « *de risque de tromperie, d'intimidation, de coercition ou de conséquences négatives importantes s'il ne donne pas son consentement* »²⁰⁹. À cet égard, le droit européen précise que le consentement n'est pas considéré comme ayant été donné librement « *si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice* »²¹⁰. Ainsi, un consentement apparaissant comme une portion non négociable des conditions générales est considéré comme non-valable²¹¹.

Deuxièmement, le consentement doit être *spécifique* à la finalité du traitement, ce qui implique qu'un consentement propre doit à nouveau être réclamé à chaque fois que la finalité poursuivie diffère de la finalité initiale²¹². Ainsi, dans l'hypothèse où le traitement poursuit plusieurs finalités, il est nécessaire que le consentement soit donné pour chacune d'elles²¹³. L'exigence d'un consentement spécifique vise à protéger l'internaute d'un éventuel

²⁰⁷ GROUPE DE TRAVAIL « ARTICLE 29 », Lignes directrices 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. 4.

²⁰⁸ Y. POULLET, « Consentement et RGPD : des zones d'ombre ! », *D.C.C.R.*, 2019/1-2, n° 122-123, p. 6.

²⁰⁹ AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, *op. cit.*, p. 159.

²¹⁰ RGPD, considérant n° 42.

²¹¹ GROUPE DE TRAVAIL « ARTICLE 29 », Lignes directrices sur le consentement au sens du règlement 2016/679, *op. cit.*, p. 6.

²¹² Y. POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.*, p. 7.

²¹³ RGPD, considérant n° 32.

détournement d'usage, qui se définit comme « *l'élargissement ou l'estompement progressif des fins auxquelles les données sont traitées, après qu'une personne concernée ait donné son consentement à la collecte initiale de ses données* »²¹⁴.

Troisièmement, l'exigence d'un consentement *éclairé* suppose que la personne concernée reçoive une information avant de prendre sa décision, et ce « *sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples* »²¹⁵. L'information en question se compose d'un certain nombre d'éléments pertinents, tels que « *l'identité du responsable du traitement et les finalités du traitement auquel sont destinées les données à caractère personnel* »²¹⁶, l'objectif étant de permettre aux individus de « *prendre des décisions en toute connaissance de cause et de comprendre ce à quoi ils consentent* »²¹⁷.

Enfin, le consentement doit être *univoque*, et pour reprendre les termes du RGPD, il doit être manifesté « *par une déclaration ou un acte positif clair* », ce qui veut dire que la personne concernée doit avoir posé un « *geste délibéré et actif* »²¹⁸. En d'autres termes, il ne doit subsister aucun doute raisonnable quant au fait que l'individu souhaitait donner son accord au traitement de ses données²¹⁹.

Il est toutefois utile de souligner que le consentement peut être retiré à tout moment²²⁰, ce qui confirme le fait qu'il s'agit d'une « *décision réversible et qu'un certain degré de contrôle par la personne concernée demeure* »²²¹. En outre, la disposition ajoute qu'il devrait être aussi simple de retirer que de donner son consentement, ce qui laisse supposer qu'« *il ne devrait exister ni obligation de motiver le retrait du consentement, ni risque de conséquences dommageables, outre la cessation des avantages qui pouvaient découler de l'utilisation des*

²¹⁴ GROUPE DE TRAVAIL « ARTICLE 29 », Lignes directrices sur le consentement au sens du règlement 2016/679, *op. cit.*, p. 13.

²¹⁵ RGPD, art. 7, § 2.

²¹⁶ RGPD, considérant n° 42.

²¹⁷ GROUPE DE TRAVAIL « ARTICLE 29 », Lignes directrices sur le consentement au sens du règlement 2016/679, *op. cit.*, p. 14.

²¹⁸ *Ibid.*, p. 18.

²¹⁹ AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, *op. cit.*, p. 166.

²²⁰ RGPD, art. 7, § 3.

²²¹ GROUPE DE TRAVAIL « ARTICLE 29 », Lignes directrices sur le consentement au sens du règlement 2016/679, *op. cit.*, p. 5.

*données à laquelle il avait été consenti »*²²².

L'article 7, paragraphe 1 du RGPD souligne que la charge de la preuve repose sur le responsable du traitement²²³. En pratique, c'est donc à Facebook qu'il revient de démontrer qu'un consentement a bel et bien été donné et que ce consentement rencontre toutes les exigences de qualité imposées par le RGPD²²⁴.

Le cumul d'autant d'impératifs pour s'assurer un consentement valable de la part de l'internaute n'est pas sans poser question. En effet, si d'autres législations protectrices, en particulier du consommateur, requièrent également l'obtention d'un consentement, aucune n'impose autant d'exigences qualitatives à ce dernier²²⁵. Il faut reconnaître que réclamer des qualités aussi nombreuses semble vain. Une brève comparaison avec la réalité du terrain suffit d'ailleurs à rapidement prendre conscience du fait que sur la toile, très peu des consentements exprimés, voire aucun, ne remplissent les conditions légales²²⁶.

Sur ce point, Y. POULLET est d'avis que *« à ce consentement individuel, il serait préférable [...] de réclamer une négociation collective [...] qui fixerait ce qui est acceptable, ce qui est exclu et les marges de manœuvre laissées au prestataire et, peut-être au consentement individuel »*²²⁷. Une telle solution nous paraît également plus profitable à la protection des consommateurs, bien plus que la forme du consentement actuellement requise, bien souvent illusoire.

§2. L'intérêt légitime

L'article 6, paragraphe 1, point f), du RGPD dispose que des données à caractère personnel peuvent faire l'objet d'un traitement licite s'il *« est 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 [...] »*.

²²² AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, op. cit., p. 167.

²²³ Et ce, en vertu du principe d'« *accountability* », que nous détaillerons dans la prochaine Section, § 7.

²²⁴ Y. POULLET, « Consentement et RGPD : des zones d'ombre ! », op. cit, p. 9.

²²⁵ *Ibid.*, p. 10.

²²⁶ *Ibid.*

²²⁷ *Ibid.*

Un intérêt est considéré comme légitime s'il réunit trois conditions : il doit « *être licite (c'est-à-dire conforme au droit en vigueur dans l'Union et dans le pays concerné) ; être formulé en termes suffisamment clairs pour permettre l'application du critère de mise en balance avec l'intérêt et les droits fondamentaux de la personne concernée (c'est-à-dire suffisamment précis) ; et constituer un intérêt réel et présent (c'est-à-dire non hypothétique)* »²²⁸.

Toutefois, ce n'est pas parce que le responsable de traitement peut se prévaloir d'un tel intérêt légitime²²⁹ qu'il peut systématiquement invoquer la disposition légale précitée comme fondement juridique à l'appui de son traitement²³⁰. Il ne s'agit en réalité que du point de départ : une fois les intérêts du responsable de traitement mis en évidence, il est question de mettre en balance ceux-ci avec les intérêts ou les libertés et droits fondamentaux de la personne concernée, afin de déterminer quels intérêts prévalent²³¹.

S'il s'avère finalement que les droits de la personne concernée l'emportent sur les intérêts légitimes du responsable de traitement, il reste à ce dernier la possibilité de « *prendre des mesures et de mettre en œuvre des garanties afin de s'assurer que l'impact sur les droits de la personne concernée est limité au minimum, et inverser l'« équilibre » avant de pouvoir invoquer légalement ce fondement légitime pour justifier le traitement* »²³².

Au regard des exigences plus nombreuses mais surtout plus strictes quant à l'application du consentement, on peut dès lors aisément comprendre que l'intérêt légitime est privilégié par les responsables de traitement lorsque ces derniers doivent opérer le choix de la base juridique sur laquelle justifier la licéité du traitement²³³.

²²⁸ GROUPE DE TRAVAIL « ARTICLE 29 », Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, WP 217, 9 avril 2014, (844/14/FR), p. 28.

²²⁹ Dans l'exposé des motifs du RGPD, au considérant n° 47, le législateur cite d'ailleurs plusieurs illustrations de ce qui constitue un intérêt légitime, comme par exemple le traitement de données à caractère personnel aux fins de prospection ou de prévention de la fraude.

²³⁰ GROUPE DE TRAVAIL « ARTICLE 29 », Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, *op. cit.*, p. 28.

²³¹ *Ibid.*, pp. 26-27.

²³² AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, *op. cit.*, p. 173.

²³³ C. PONSART ET R. ROBERT, « Le règlement européen de protection des données personnelles », *op. cit.*, p. 425.

Il reste que l'article 6 du RGPD et l'obligation inhérente de licéité du traitement ne dispensent pas le responsable de traitement de respecter l'article 5 qui liste les principes de base relatifs au traitement de données à caractère personnel²³⁴, que nous allons découvrir ci-dessous.

Section 2. Les principes de base relatifs au traitement de données à caractère personnel

L'ensemble des principes s'appliquant à la protection des données est listé à l'article 5 du RGPD : le principe de licéité, loyauté et transparence ; le principe de limitation des finalités ; le principe de minimisation des données ; le principe d'exactitude ; le principe de limitation de la conservation ; le principe d'intégrité et confidentialité ; et enfin, le principe de responsabilité. En effet, il est indispensable d'analyser ces principes car leur violation est notamment susceptible de constituer une pratique interdite au sens du livre VI du Code de droit économique belge.

§1. Principes de licéité, de loyauté et de transparence du traitement

Comme nous l'avons vu, le droit de l'Union impose tout d'abord que le traitement de données à caractère personnel soit licite, c'est-à-dire qu'il soit fondé sur l'une des six bases juridiques de l'article 6, paragraphe 1 du RGPD.

Outre la licéité du traitement, le traitement est encadré par le principe de loyauté, qui requiert des responsables de traitement qu'ils informent les personnes concernées du fait qu'ils vont traiter leurs données (c'est-à-dire que le traitement ne doit pas être gardé secret) et que, autant que faire se peut, ils vont « *agir de façon à se conformer rapidement aux souhaits de la personne concernée, en particulier quand son consentement constitue la base juridique du traitement des données* »²³⁵.

²³⁴ Y. POULLET, « Consentement et RGPD : des zones d'ombre ! », *op. cit.*, p. 18.

²³⁵ AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, *op. cit.*, p. 132.

Enfin, bien qu'il ne soit pas défini²³⁶ (même s'il est longuement détaillé dans le considérant numéro 39 du RGPD), le principe de transparence prescrit que la collecte et l'utilisation des données doit avoir lieu en toute transparence vis-à-vis des personnes concernées. Les articles 12 à 14 du RGPD mentionnent la qualité et le contenu des informations qui doivent être fournies aux internautes, notamment le fait « *qu'elles doivent être concises, transparentes, compréhensibles et aisément accessibles, en des termes clairs et simples, [...] et fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique* »²³⁷.

§2. Principe de limitation des finalités

Mis en avant depuis de nombreuses années comme le principe fondamental de la protection des données, le « *principe de finalité* » dans son appellation la plus courante, pose l'exigence que les données soient « *collectées pour des finalités déterminées, explicites et légitimes, et ne soient pas traitées ultérieurement de manière incompatible avec ces finalités* »²³⁸. En d'autres termes, dès le départ, il est indispensable que l'étendue des opérations du traitement soit délimitée et exprimée de manière claire et sans ambiguïté²³⁹. Ce n'est qu'une fois qu'il aura respecté ces exigences que le responsable de traitement aura la possibilité d'effectuer sur les données n'importe quelle opération qui s'avèrerait compatible avec les finalités d'origine²⁴⁰.

Dans la pratique, de nombreuses interrogations ont surgi au sujet de la notion d'utilisation « *compatible* », c'est pourquoi les auteurs du RGPD ont décidé d'en délimiter les contours à l'aide d'une liste de critères qui permettent de vérifier la compatibilité du traitement de données entre la finalité initiale et la finalité nouvelle²⁴¹. Les facteurs à prendre en compte sont notamment : le lien qui existerait entre les finalités prévues et les finalités envisagées ; le contexte dans lequel les données à caractère personnel ont été collectées, en

²³⁶ GROUPE DE TRAVAIL « ARTICLE 29 », Lignes directrices sur le consentement au sens du règlement 2016/679, *op. cit.*, p. 6.

²³⁷ RGPD, art. 12, § 1^{er}.

²³⁸ RGPD, art. 5, § 1^{er}, b).

²³⁹ WORKING PARTY « ARTICLE 29 », Opinion 03/2013 on purpose limitation, WP 203, 2 April 2013, (00569/13/EN), p. 12.

²⁴⁰ AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, *op. cit.*, p. 138.

²⁴¹ C. DE TERWANGNE, K. ROSIER et B. LOSDYCK, « Le règlement européen relatif à la protection des données à caractère personnel : quelles nouveautés ? », *op. cit.*, p. 305.

particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ; la nature des données, ordinaires ou sensibles ; les conséquences potentielles du traitement ultérieur ; et finalement, les garanties existantes²⁴².

En outre, il est important d'attirer l'attention sur le fait qu'il est autorisé, dans deux hypothèses distinctes, de traiter les données pour une finalité différente que la finalité pour lesquelles elles ont été collectées, et ce sans devoir vérifier la compatibilité entre les deux finalités : lorsque la personne concernée donne son consentement pour le traitement ultérieur, et lorsque le traitement est fondé sur le droit européen ou sur le droit national²⁴³.

§3. Principe de minimisation des données

En vertu du principe de minimisation, les données utilisées lors d'un traitement doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* »²⁴⁴. Le considérant numéro 39 du RGPD précise que le critère de nécessité se rapporte tant à la quantité qu'à la qualité des données traitées, mais également à la durée de leur conservation²⁴⁵, qui doit également être « *limitée au strict minimum* ».

Dès lors, s'il est évident qu'un traitement d'une quantité excessive de données²⁴⁶ est interdit, il n'est pas non plus autorisé d'opérer un traitement d'une seule et unique donnée qui porterait excessivement atteinte à l'individu concerné²⁴⁷.

²⁴² RGPD, art. 6, § 4. Voy. également RGPD, considérant n° 50.

²⁴³ C. DE TERWANGNE, K. ROSIER et B. LOSDYCK, « Le règlement européen relatif à la protection des données à caractère personnel : quelles nouveautés ? », *op. cit.*, p. 305.

²⁴⁴ RGPD, art. 5, § 1^{er}, c).

²⁴⁵ C. PONSART ET R. ROBERT, « Le règlement européen de protection des données personnelles », *op. cit.*, p. 424.

²⁴⁶ En ce sens, voy. l'explication de la notion de données « *excessives* » dans CONVENTION N° 108 DU CONSEIL DE L'EUROPE, *Projet de rapport explicatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, version du 2 juin 2016 (disponible à l'adresse suivante <https://rm.coe.int/convention-pour-la-protection-des-personnes-a-l-egard-du-traitement-au/16806b6ec3>, page consultée le 5 juillet 2020) : « Cette disposition vise aussi bien les aspects quantitatifs que qualitatifs des données à caractère personnel. Des données qui seraient adéquates et pertinentes mais entraîneraient une ingérence disproportionnée dans les droits et libertés fondamentaux en jeu doivent être considérées comme excessives et ne pas être traitées ».

²⁴⁷ C. DE TERWANGNE, K. ROSIER et B. LOSDYCK, « Le règlement européen relatif à la protection des données à caractère personnel : quelles nouveautés ? », *op. cit.*, p. 305.

Enfin, selon le principe de minimisation des données, un traitement de données à caractère personnel ne peut être réalisé que s'il n'est raisonnablement pas possible d'atteindre la finalité sans celui-ci²⁴⁸.

§4. Principe d'exactitude des données

L'article 5, paragraphe 1^{er}, point d) du RGPD énonce le principe d'exactitude selon lequel les données doivent être « *exactes et si nécessaires, tenues à jour* ». En ce sens, la disposition ajoute que toutes les mesures raisonnables doivent être prises afin de garantir que les données inexactes ou incomplètes soient effacées ou rectifiées sans délai. Dès lors, il peut s'avérer nécessaire, pour le responsable de traitement, de vérifier et de mettre à jour régulièrement les données, afin de garantir leur exactitude et ce, de manière continue²⁴⁹.

Par conséquent, l'exigence d'exactitude semble à la fois recouvrir une obligation de résultat, lorsque la personne concernée communique une demande de rectification²⁵⁰, et une obligation de moyens, en vertu de laquelle le responsable du traitement doit instaurer des mesures raisonnables de façon à actualiser les données qu'il traite²⁵¹.

§5. Principe de limitation de la conservation

L'article 5, paragraphe 1, point e), du RGPD impose que les données à caractère personnel soient « *conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées* ». En pratique, les données doivent donc être supprimées ou anonymisées lorsque les finalités dont il est question ont été atteintes²⁵².

²⁴⁸ RGPD, considérant n° 39.

²⁴⁹ AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, op. cit., p. 142.

²⁵⁰ RGPD, art. 16.

²⁵¹ Par exemple, en s'assurant, lors des contacts avec ses clients, que leurs coordonnées sont toujours correctes. Voy. en ce sens C. PONSART ET R. ROBERT, « Le règlement européen de protection des données personnelles », op. cit., p. 424.

²⁵² AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, op. cit., p. 144.

Ainsi, le RGPD²⁵³ conseille au responsable du traitement de « *fixer des délais pour l'effacement des données qui ne seraient plus nécessaires ou, à tout le moins, pour un examen périodique* »²⁵⁴.

§6. Principe d'intégrité et de confidentialité des données

Également connu sous le nom de « *principe de sécurité* »²⁵⁵, le principe d'intégrité et de confidentialité impose que des mesures techniques ou organisationnelles appropriées soient mises en place lors du traitement de données à caractère personnel, afin de les protéger dans l'hypothèse d'un accès, d'une utilisation, d'une modification, d'une divulgation, d'une perte, d'une destruction ou d'un dommage accidentel, non autorisé ou illicite²⁵⁶.

Plus largement développé dans une des sections du chapitre consacré aux responsables et sous-traitants²⁵⁷, le principe de sécurité requiert notamment que ces derniers adoptent des mesures de sécurité adaptées aux risques existants²⁵⁸. En ce sens, le caractère approprié des mesures mises en place doit être déterminé au cas par cas²⁵⁹ et faire l'objet d'un réexamen régulier²⁶⁰.

§7. Principe de responsabilité (“accountability”)

L'article 5, paragraphe 2 du RGPD énonce le dernier principe de base relatif au traitement de données à caractère personnel, selon lequel le responsable du traitement est responsable du respect de l'ensemble des exigences vues dans la présente section, et doit être en mesure de le démontrer.

²⁵³ RGPD, considérant n° 39.

²⁵⁴ C. PONSART ET R. ROBERT, « Le règlement européen de protection des données personnelles », *op. cit.*, p. 424.

²⁵⁵ AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, *op. cit.*, p. 146.

²⁵⁶ RGPD, art. 5, § 1^{er}, f) et considérant n° 39.

²⁵⁷ RGPD, articles 32 à 34 faisant partie de la Section II du chapitre IV consacré aux devoirs des responsable et sous-traitant.

²⁵⁸ RGPD, art. 32.

²⁵⁹ Le responsable du traitement et le sous-traitant devraient ainsi tenir compte « *de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques* » (RGPD, art. 32, § 1^{er}).

²⁶⁰ AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, *op. cit.*, p. 146.

Section 3. Les obligations du responsable de traitement

§1. Mise en pratique du principe de responsabilité (“accountability”)

Même si le principe de responsabilité est déjà repris à l'article 5, paragraphe 2, du RGPD en tant que principe fondamental en matière de protection des données, c'est vers l'article 24 qu'il faut se tourner pour avoir une meilleure compréhension du concept une fois qu'il faut le mettre en œuvre²⁶¹. En effet, la disposition énonce les deux composantes de base du principe d'« *accountability* » puisqu'elle prévoit que « [...] *le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement* »²⁶².

Premièrement, le responsable de traitement est donc chargé de mettre en œuvre, de manière active et continue, les mesures techniques et organisationnelles appropriées, dans le but de promouvoir et garantir la protection des données lors de ses activités de traitement²⁶³.

Le G29 précise que « *le type de procédures et de mécanismes varierait selon les risques que posent le traitement et la nature des données* »²⁶⁴. Ainsi, le responsable de traitement peut se conformer au principe d'*accountability* à l'aide de différentes méthodes, notamment : en tenant un registre des activités de traitement effectuées et en le mettant à la disposition de l'autorité de contrôle sur demande²⁶⁵ ; dans certains cas, en désignant un délégué à la protection des données, qui est associé à toutes les questions relatives à la protection des données à caractère personnel²⁶⁶ ; en réalisant une analyse d'impact relative à la protection des données lorsqu'un type de traitement est susceptible d'engendrer un risque

²⁶¹ A. DELFORGE, « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.*, p. 383.

²⁶² Les termes « *met en œuvre* » et « *démontrer* » sont soulignés par nos soins.

²⁶³ AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, *op. cit.*, p. 150.

²⁶⁴ GROUPE DE TRAVAIL « ARTICLE 29 », Avis 3/2010 sur le principe de responsabilité, WP 173, 13 juillet 2010, (00062/10/FR), p. 2.

²⁶⁵ RGPD, art. 30.

²⁶⁶ RGPD, art. 37 à 39.

élevé pour les droits et libertés des personnes physiques²⁶⁷ ; ou encore en adhérant à un code de conduite ou à un mécanisme de certification approuvé²⁶⁸.

Deuxièmement, le responsable du traitement doit pouvoir attester du fait qu'il respecte les principes et obligations du RGPD, et ce, à tout moment, que ce soit aux personnes concernées ou aux autorités de contrôle²⁶⁹. Par conséquent, le principe de responsabilité exige du responsable du traitement qu'il démontre activement une conformité, et pas seulement qu'il se contente d'attendre passivement que les personnes concernées ou les autorités de contrôle signalent des irrégularités²⁷⁰.

Bien que le RGPD ne prévoie aucune sanction administrative pour la violation de l'article 24, la violation du principe d'« *accountability* » peut quant à elle conduire à de lourdes sanctions²⁷¹, à charge pour la victime qui souhaiterait réclamer le dédommagement du préjudice qu'elle a subi d'en apporter la preuve²⁷².

Enfin, une précision notable doit être mise en avant : bien que le principe de responsabilité ne s'adresse en apparence qu'aux responsables du traitement, les sous-traitants sont également considérés comme tels, dans la mesure où ils doivent se conformer à plusieurs obligations et entretiennent une relation directe avec la responsabilité²⁷³.

§2. Deux obligations pour tout traitement : le “privacy by design” et le “privacy by default”

Certaines « *mesures techniques et organisationnelles* » décrites ci-dessus sont facultatives et dépendent du bon vouloir du responsable de traitement, ce qui n'est toutefois

²⁶⁷ RGPD, art. 35.

²⁶⁸ RGPD, art. 40 et 42.

²⁶⁹ C. PONSART ET R. ROBERT, « Le règlement européen de protection des données personnelles », *op. cit.*, p. 424.

²⁷⁰ AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, *op. cit.*, p. 154.

²⁷¹ RGPD, art. 83, § 5, a).

²⁷² A. DELFORGE, « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.*, p. 386.

²⁷³ AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, *op. cit.*, p. 150.

pas le cas des deux notions de “*privacy*” qui sont obligatoires pour tout traitement²⁷⁴, et qui se révèlent particulièrement pertinentes dans le cadre de notre analyse.

Trop souvent considérée comme une étape supplémentaire lors d’un traitement de données, la protection de la vie privée est dorénavant au centre des préoccupations grâce à un changement radical de point de vue : l’importance accordée à la question est désormais présente dès la conception du traitement, plutôt qu’*a posteriori*²⁷⁵.

A. “*Privacy by design*”

Le principe de la protection des données par défaut, énoncé à l’article 25 du RGPD, requiert que « *les paramètres de respect de la vie privée dans les services et produits soient par défaut conformes aux principes généraux de la protection des données* »²⁷⁶. En d’autres termes, il véhicule l’idée selon laquelle le responsable de traitement doit adopter un cadre normatif interne et organiser des mesures qui respectent spécialement les principes de protection des données et ce, dès la conception du traitement²⁷⁷.

Les mesures en question peuvent notamment viser « *à réduire à un minimum le traitement des données à caractère personnel, à pseudonymiser les données à caractère personnel dès que possible, à garantir la transparence en ce qui concerne les fonctions et le traitement des données à caractère personnel, à permettre à la personne concernée de contrôler le traitement des données, à permettre au responsable du traitement de mettre en place des dispositifs de sécurité ou de les améliorer* »²⁷⁸.

Ainsi, l’objectif qui se cache derrière le principe de “*privacy by design*” est de faire peser encore davantage la responsabilité du respect de la vie privée sur les épaules des entreprises, en les obligeant à tenir compte de la législation sur la protection des données dès

²⁷⁴ A. DELFORGE, « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.*, p. 384.

²⁷⁵ *Ibid.*, pp. 386-387.

²⁷⁶ A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 307.

²⁷⁷ A. BAMDE, *Le Droit dans tous ses états - RGPD : les concepts de privacy by design et de privacy by default*, 22 décembre 2018 (disponible sur <https://aurelienbamde.com/2018/12/22/rgpd-les-concepts-de-privacy-by-design-et-de-privacy-by-default/>, page consultée le 05 juillet 2020).

²⁷⁸ RGPD, considérant n° 78.

la conception du profilage²⁷⁹. Toutefois, il ne faut pas oublier le rôle que les individus doivent eux-mêmes jouer, que ce soit en s'assurant de la bonne configuration de leur ordinateur, en installant une extension, ou encore en utilisant des logiciels anti-traçage²⁸⁰.

B. “Privacy by default”

Comme son nom l'indique, le concept de vie privée par défaut, également énoncé à l'article 25 du RGPD, consiste à « *instaurer une configuration des paramètres de confidentialité par défaut, dès l'inscription à un service en ligne* »²⁸¹. Autrement dit, il revient au responsable de traitement d'assurer, par défaut, le niveau de protection le plus élevé possible et ce, grâce à des mesures de sécurité et de protection installées systématiquement en cas de traitement portant sur des données à caractère personnel²⁸².

Pour les mesures prises au titre du “*privacy by default*”, on renvoie aux développements ci-dessus (le principe de “*privacy by default*” n'étant finalement qu'une forme particulière du principe de “*privacy by design*”)²⁸³, en ajoutant cependant une précision notable : le responsable de traitement doit en particulier offrir la garantie que, par défaut, les données d'une personne ne seront jamais rendues publiques (c'est-à-dire accessibles à un nombre indéterminé de personnes physiques) sans une intervention active de la personne concernée qui autoriserait le contraire²⁸⁴.

En pratique, pour prendre l'exemple de Facebook, qui prévoit que chaque profil d'utilisateur peut être soit « *privé* » (non accessible à des tiers), soit « *semi-privé* » (accessible à certaines personnes autorisées par l'internaute), soit « *public* » (accessible à tous les membres du réseau social)²⁸⁵, il faudrait que le profil soit paramétré *par défaut* en mode

²⁷⁹ A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 307.

²⁸⁰ *Ibid.*

²⁸¹ *Ibid.*, pp. 306-307.

²⁸² A. BAMDE, *Le Droit dans tous ses états - RGPD : les concepts de privacy by design et de privacy by default*, *op. cit.*

²⁸³ A. DELFORGE, « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.*, p. 391.

²⁸⁴ RGPD, art. 25, § 2 *in fine*.

²⁸⁵ Voy. Facebook, *Paramètres et outils de confidentialité – Votre activité et Comment les autres peuvent vous trouver et vous contacter*, (disponible sur : <https://www.facebook.com/settings?tab=privacy>, page consultée le 5 juillet 2020).

« *privé* », avec la possibilité pour l'internaute, s'il désire partager plus ou moins largement certaines informations, de configurer selon ses goûts les paramètres de son profil²⁸⁶.

À l'heure actuelle, c'est encore et toujours la configuration inverse qui est prévue sur la plateforme, c'est-à-dire que le profil est réglé par défaut en mode « *public* », laissant à l'utilisateur le soin de trouver lui-même dans les paramètres de son compte la manière de restreindre la diffusion de ses informations personnelles²⁸⁷. Il va de soi que cela pose un réel problème de transparence, car rares sont les personnes à être au courant de la publicité qui est faite de leurs données, et plus rares encore sont les personnes à prendre le temps de rectifier les paramètres par défaut²⁸⁸.

Dans le même ordre d'idée, Facebook avait modifié de manière unilatérale la charte de ses conditions d'utilisation aux fins d'organiser une licence perpétuelle et mondiale. Celle-ci aurait dû lui permettre de conserver et de se servir de tous les contenus produits par ses utilisateurs, et ce, même une fois ces derniers désinscrits de la plateforme. Ainsi, l'on pouvait lire dans l'onglet « *Droit de propriété* » du contenu du site²⁸⁹, le paragraphe suivant : « *Vous accordez à Facebook le droit irrévocable, perpétuel, non-exclusif, transférable mondialement d'utiliser, copier, publier, diffuser, stocker, exécuter, transmettre, scanner, modifier, éditer, traduire, adapter, redistribuer n'importe quel contenu déposé sur le site* »²⁹⁰.

Néanmoins, le projet fût rapidement abandonné par le réseau social, qui fit volte-face. Après une réaction tranchée de la part des internautes, lesquels dénonçaient une atteinte à leur

²⁸⁶ A. DELFORGE, « Titre 8 - Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.*, p. 391.

²⁸⁷ *Ibid.*

²⁸⁸ L'inconscience générale pourrait notamment provenir du fait qu'il est difficile d'avoir accès aux paramètres de confidentialité, et qu'il est encore plus difficile pour l'internaute de comprendre comment les régler à sa convenance. Voy. en ce sens F. MEURICE, Head of Digital Service Design, interview réalisée par M.-E. RODRIGUEZ le 30 juillet 2020, p. 84 : « *Aujourd'hui, il est très compliqué pour un utilisateur lambda d'aller bloquer tous ses paramètres pour être sûr de ne communiquer qu'avec ses amis ou sa famille. En fait, j'ai vérifié et lorsque Facebook a été lancé (pour ma part j'y suis inscrite depuis 2007), il était facile de créer des groupes d'utilisateurs et de cacher tout son contenu. J'acceptais quelqu'un et systématiquement, Facebook me proposait de le mettre dans une catégorie, comme par exemple la catégorie des gens avec lesquels je désire uniquement partager ma photo de profil, mon nom et mon prénom* ».

²⁸⁹ En ce sens, voy. notamment Facebook, *Politique d'utilisation des données* (disponible sur <https://www.facebook.com/privacy/explanation>, page consultée le 20 juillet 2020) et Facebook, *Propriété intellectuelle* (disponible sur https://www.facebook.com/help/intellectual_property, page consultée le 20 juillet 2020).

²⁹⁰ A. CONFOLANT, *Licence perpétuelle des données : Facebook fait volte-face*, 18 février 2009 (disponible sur <https://www.itespresso.fr/licence-perpetuelle-des-donnees-facebook-fait-volte-face-24411.html>, page consultée le 10 novembre 2019).

vie privée et à leurs données personnelles²⁹¹, Mark Zuckerberg – fondateur et PDG du site américain – publia quelques mots sur son blog officiel pour tenter de calmer les ardeurs et de ne pas se mettre à dos les 175 millions de membres à l’époque : « *Nous ne voudrions pas partager vos informations d’une façon qui ne vous conviendrait pas* »²⁹². En définitive, Facebook n’eut pas d’autre choix que de faire machine arrière et d’annuler la licence perpétuelle, pour en revenir à la licence limitée auparavant mise en place.

²⁹¹ En effet, suite au sondage réalisée par le réseau social à propos de cette modification contractuelle, le résultat fût sans appel : seuls 6% des utilisateurs avaient déclaré être en faveur de la nouvelle mesure. Voy. en ce sens O. ROBILLART, *Documents personnels : Facebook renonce à la licence perpétuelle*, 18 février 2009 (disponible sur <https://www.silicon.fr/documents-personnels-facebook-renonce-a-la-licence-perpetuelle-34112.html>, page consultée le 11 novembre 2019).

²⁹² LA DERNIERE HEURE, *Facebook rassure ses utilisateurs*, 17 février 2009 (disponible sur <https://www.dhnet.be/actu/new-tech/facebook-rassure-ses-utilisateurs-51b7b33fe4b0de6db9889213>, page consultée le 11 novembre 2019).

Titre 3. Mieux protéger ses données sur Internet

Chapitre 1. Une meilleure sensibilisation des individus

Section 1. Aperçu de quelques actions préventives possibles

Face à l'univers numérique globalisé et en perpétuel progrès qui nous entoure, une attitude à adopter pourrait être de miser sur des actions préventives, dont l'objectif serait de conscientiser les citoyens face aux menaces qui existent lorsqu'ils surfent sur Internet²⁹³.

§1. Campagnes de sensibilisation et outils pédagogiques

Dans un premier temps, l'idée serait d'organiser des campagnes de sensibilisation visant à partager aux utilisateurs des informations, notamment quant à la collecte des données à caractère personnel, aux finalités poursuivies par les responsables de traitement, à la durée de conservation de ces mêmes données ainsi qu'aux démarches à suivre en vue d'effacer ces dernières²⁹⁴.

Ainsi, il serait par exemple question de mettre en place « *la même chose que la sécurité routière qui, par des vidéos choquantes, éduque les gens. En Suisse, ils sont très forts là-dedans, ils publient des vidéos où tu es complètement bluffé. Selon moi, c'est vraiment le rôle de l'État, du législateur et des entreprises de lancer ce genre de campagnes-là. [...] Il y a également trop peu de reportages qui sont intéressants, bien faits et surtout accessibles* »²⁹⁵.

La mise en œuvre d'outils pédagogiques permettrait également d'apprendre des techniques de protection pour protéger sa vie privée, mais aussi pour celles des personnes qui nous entourent. Particulièrement chez les plus jeunes, leurs premiers clics sur le Net devraient s'appuyer sur ce type d'instruments. Plus les gens seront au courant des risques, mieux ils

²⁹³ A. ARAMAZANI, « Le droit à l'oubli et internet », *op. cit.*, p. 48.

²⁹⁴ *Ibid.*

²⁹⁵ Voy. en ce sens F. MEURICE, Head of Digital Service Design, interview réalisée par M.-E. RODRIGUEZ le 30 juillet 2020, p. 86

sauront gérer les conséquences néfastes qui peuvent surgir à propos de leurs données à caractère personnel²⁹⁶.

L'on souligne qu'il existe d'ores et déjà des projets qui ont pour objectif d'attirer l'attention des internautes sur les bons gestes à adopter lorsqu'ils naviguent sur Internet, tel que le programme « *Internet sans crainte* »²⁹⁷.

§2. Configuration du navigateur, destructeur de cookies et bloqueur de publicité

Dans un deuxième temps, il serait judicieux d'encourager les internautes à configurer leur navigateur Internet avec plus de soin²⁹⁸. Pour les plus habiles, il est également possible de se servir d'un proxy, serveur intermédiaire entre l'individu et le réseau, qui permet de naviguer anonymement sur la toile²⁹⁹.

Une autre piste à creuser pour l'internaute serait d'accroître sa vigilance afin que les cookies et autres technologies similaires n'envahissent pas ses appareils pour capter ses données. Pour ce faire, le premier réflexe à adopter serait de désactiver l'acceptation automatique sur le navigateur Internet utilisé³⁰⁰. Plusieurs inconvénients notables viennent toutefois ternir le paysage, et pour n'en citer que quelques-uns : détruire l'ensemble des cookies³⁰¹ après leur installation obligerait en fin de compte l'utilisateur à recommencer l'opération pour les réinstaller, bloquer tous les cookies pourrait s'avérer pénalisant pour la navigation, la suppression des cookies à chaque session ne serait guère pratique, en plus d'être pénible³⁰², etc.

²⁹⁶ A. ARAMAZANI, « Le droit à l'oubli et internet », *op. cit.*, p. 48.

²⁹⁷ *Internet sans crainte : un programme national et européen* (disponible sur <https://www.internetsanscrainte.fr/projet>, page consultée le 19 novembre 2019).

²⁹⁸ A. ARAMAZANI, « Le droit à l'oubli et internet », *op. cit.*, p. 48.

²⁹⁹ CRUQUENAIRE A., DEMOULIN M., GOBERT D., LAZARO C., MARTHOZ B., MONTERO E., ROBERT R. et VAN DER PERRE A., « Partie 4. Se protéger des « agressions » sur Internet », in *Guide pour les utilisateurs d'Internet, rédigé par le Centre de Recherches Informatique et Droit (FUNDP – Namur) dans le cadre d'un contrat de recherches financé par le Service public fédéral Économie, P.M.E., Classes moyennes et Énergie*, (Sous la dir. de DEMOULIN M.), Bruxelles, Regis Massant, 2011, pp. 109-113.

³⁰⁰ *Ibid.*

³⁰¹ Il existe en effet des « destructeurs de cookies », comme par exemple le programme « *Cookies Manager* », téléchargeable gratuitement.

³⁰² A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 305.

Par ailleurs, il existe également des logiciels capables de bloquer la publicité³⁰³, qu'elle soit ciblée ou pas, avec pour certains d'entre eux une fonctionnalité supplémentaire anti-tracking³⁰⁴, toujours dans l'idée de surfer anonymement sur Internet.

§3. Anonymat et pseudonymat

Dans un troisième temps, une option intéressante pourrait être d'inciter les internautes à recourir au pseudonymat ou à l'anonymat lorsque cela s'avère utile³⁰⁵.

A. Données anonymisées : une garantie suffisante ?

Une donnée anonymisée se caractérise par le fait que « *tous les éléments identifiants ont été supprimés d'un ensemble de données à caractère personnel* »³⁰⁶. Plus précisément, les informations collectées ne doivent plus contenir aucune trace qui soit susceptible, à l'aide d'un effort raisonnable, de permettre la ré-identification de la ou des personnes concernées³⁰⁷. En d'autres termes, l'identification ne doit plus être possible et ce, de manière irréversible.

Une fois les données correctement anonymisées, elles ne sont plus considérées comme des données à caractère personnel³⁰⁸. Dès lors, puisque les données anonymisées ne peuvent plus être rattachées à une personne individualisée, la législation sur la protection des données n'a plus vocation à s'appliquer³⁰⁹.

Néanmoins, il convient de rester sur ses gardes à l'égard des techniques d'anonymisation, car comme le souligne très justement le G29, le risque d'identification fait

³⁰³ C'est notamment le cas du programme « *Ad block* ». Voy. en ce sens *Adblock Plus : surfez sur Internet sans publicités agaçantes* (disponible sur <https://adblockplus.org/>, page consultée le 19 novembre 2019)

³⁰⁴ Par exemple, le mécanisme « *Do Not Track* » permet de signaler aux sites Internet le refus des utilisateurs de faire l'objet d'un suivi en ligne. Voy. en ce sens A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 305.

³⁰⁵ A. ARAMAZANI, « Le droit à l'oubli et internet », *op. cit.*, p. 48.

³⁰⁶ A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », *op. cit.*, p. 296.

³⁰⁷ RGPD, considérant n° 26.

³⁰⁸ AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, *op. cit.*, p. 106.

³⁰⁹ En effet, le RGPD, considérant n° 26 indique qu'« *il n'y a pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. Le présent règlement ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherches* ».

partie intégrante des techniques d'anonymisation, aussi minime soit-il³¹⁰. En effet, on peut facilement imaginer à quel point il est difficile de constituer un ensemble de données véritablement anonymes tout en maintenant suffisamment d'informations pour la réalisation du traitement³¹¹.

Par conséquent, il faut pouvoir reconnaître l'efficacité mais également les limites des différentes techniques d'anonymisation, en gardant à l'esprit que certaines d'entre elles ne se montrent pas nécessairement pertinentes dans tous les cas³¹². Ainsi, trouver la solution la plus optimale dans une situation problématique donnée requiert de choisir la technique appropriée au cas par cas.

Malgré tout, la possibilité d'identifier un individu grâce à des données anonymes croisées avec d'autres types de données codées ou nominatives reste ouverte. De fait, il apparaît en définitive utopique d'envisager l'existence d'un anonymat total sur Internet et de manière corolaire, de données non-personnelles³¹³.

B. Données pseudonymisées : un outil efficace ?

Les informations personnelles sont considérées comme pseudonymisées lorsque les éléments tels que le nom, la date de naissance, le sexe, l'adresse, ou encore d'autres composantes de la vie privée susceptibles de conduire à une identification, sont masqués derrière un pseudonyme³¹⁴.

La pseudonymisation peut notamment être obtenue par le chiffrement des éléments faisant partie des données à caractère personnel, le rattachement à l'identité ne résidant alors

³¹⁰ Le risque de ré-identification peut être évalué en tenant compte « des délais, efforts ou ressources nécessaires au regard de la nature des données, du contexte de leur utilisation, des techniques de ré-identification disponibles et des coûts correspondants ». Voy. en ce sens COMITE CONSULTATIF DE LA « CONVENTION 108 », Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées, T-PD(2017)01, 23 janvier 2017, § 6.2.

³¹¹ Plusieurs études ont d'ailleurs démontré la complexité du processus. Voy. en ce sens GROUPE DE TRAVAIL « ARTICLE 29 », Avis 05/2014 sur les techniques d'anonymisation, WP 216, 10 avril 2014, (0829/14/FR), p. 3.

³¹² AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, op. cit., p. 105.

³¹³ DINANT J.-M., LAZARO C., POULLET Y., LEFEVER N. ET ROUVROY A., *L'application de la Convention 108 au mécanisme de profilage : Éléments de réflexion destinés au travail du futur Comité consultatif (T-PD)*, op. cit., pp. 4-5.

³¹⁴ AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, op. cit., p. 106.

plus que dans le pseudonyme associé à une clé de chiffrement³¹⁵. Il est a priori complexe d'identifier des données pseudonymisées sans l'aide d'une clé de chiffrement, mais pour toute personne habituée à s'en servir, une ré-identification s'avère en fait facilement réalisable (c'est d'ailleurs pourquoi il est indispensable de veiller à éviter toute utilisation de clés de chiffrement par des personnes non autorisées)³¹⁶.

Ainsi, contrairement aux données anonymisées et en raison de la protection dont elles ont besoin, les données pseudonymisées restent qualifiées de données à caractère personnel et entrent donc dans le giron de la législation relative à la protection des données³¹⁷. Au final, même s'il existe toujours un risque d'identification, la pseudonymie présente l'avantage d'offrir un excellent moyen d'honorer le principe de la protection dès la conception³¹⁸.

Section 2. L'information, l'éducation et la responsabilisation des internautes

Alors que l'on place de plus en plus la protection du droit à la vie privée au centre de toutes les préoccupations, les personnes concernées manifestent généralement peu d'intérêt (voire même un désintérêt profond) à l'utilisation qui est faite de leurs données personnelles, ainsi qu'aux intrusions qui en découlent³¹⁹. Paradoxalement, lorsque l'on se tourne vers elles pour les interroger à ce sujet, chacune d'entre elles déclare vouloir protéger sa vie privée³²⁰.

Toutefois, seule une minorité d'individus ont réellement l'air de prendre conscience de l'importance de ce droit, de le faire valoir, de le faire respecter et de le revendiquer³²¹. Au contraire, la vie privée est plus que jamais exposée aux yeux de tous, notamment par le biais des réseaux sociaux, avec une participation active de ces mêmes individus, qui confirmaient

³¹⁵ AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, op. cit., p. 107.

³¹⁶ *Ibid.*

³¹⁷ AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE ET CONSEIL DE L'EUROPE, *Manuel de droit européen en matière de protection des données*, op. cit., p. 107.

³¹⁸ Comme nous l'avons précédemment étudié dans le Titre 2, Chapitre 2, Section 3, § 3 ; A. GROSJEAN, « Chapitre 4 – Le profilage : un défi pour la protection des données à caractère personnel », op. cit., p. 296.

³¹⁹ N. RAGHENO, « Droits fondamentaux et société numérique : la vie privée existe-t-elle encore ? », op. cit., p. 18.

³²⁰ *Ibid.*

³²¹ N. RAGHENO, « Droits fondamentaux et société numérique : la vie privée existe-t-elle encore ? », op. cit., p. 18.

souhaiter préserver leur part d'intimité³²². Ce n'est d'ailleurs pas un hasard si l'« *on dit souvent que la majeure partie des problèmes en « IT »*³²³ *se situent entre le clavier et la chaise* »³²⁴.

L'une des explications possibles pourrait être que « *la plupart du temps, les gens qui estiment ne rien avoir à cacher se targuent d'un cadre moral très strict : ils sont chrétiens ou conservateurs, « boomers », et assez conventionnels. Si ces personnes-là n'ont pas peur d'être exposées, c'est parce qu'elles ne sont jamais sorties du cadre bien classique de leur milieu et n'ont jamais été moquées et/ou persécutées. Ces individus ne sont pas homosexuels, ou handicapés, ou de couleur, ou d'une autre religion que le christianisme. Dès lors, ils se montrent confiants parce que les propriétaires de Facebook sont comme eux : hétérosexuels, blancs et chrétiens* »³²⁵.

Pour franchir un pas de plus dans la réflexion, l'on pourrait être amené à s'interroger sur la question de savoir ce que souhaite réellement le citoyen lorsqu'il dévoile de son propre chef et sans retenue ses données personnelles. S'il est prévenu, sans malentendu possible, sur les conséquences et la commercialisation éventuelle de ses données, est-il également nécessaire de le protéger contre lui-même³²⁶ ?

Une façon parmi d'autres d'éveiller les consciences pourrait être « *de montrer aux internautes ce que l'on sait déjà d'eux. Les gens ne se rendent pas compte de l'étendue des données collectées, mais une fois que l'on commence à parler à un inconnu du nom de ses enfants ou de sa peinture de chaussures, la prise de conscience est quasi instantanée* »³²⁷.

Il n'est pas question, en l'espèce, de sous-estimer la responsabilité qui pèse sur les responsables de traitement, quels qu'ils soient. Plus que jamais, il est indéniable qu'il faut instaurer une déontologie et un cadre légal performant, nécessités qui s'avèrent d'autant plus

³²² N. RAGHENO, « Droits fondamentaux et société numérique : la vie privée existe-t-elle encore ? », *op. cit.*, p. 18.

³²³ Les « *Information Technology* » en anglais et « *Technologies de l'information et de la communication* » (TIC) en français désignent les techniques utilisées dans le traitement et la transmission des informations.

³²⁴ F. MEURICE, Head of Digital Service Design, interview réalisée par M.-E. RODRIGUEZ le 30 juillet 2020, p. 87.

³²⁵ F. ZÖFEL, Data Protection Officer, interview réalisée par M.-E. RODRIGUEZ le 23 juillet 2020, p. 79.

³²⁶ *Ibid.*, p. 22.

³²⁷ F. ZÖFEL, Data Protection Officer, interview réalisée par M.-E. RODRIGUEZ le 23 juillet 2020, p. 79.

indispensables que les hypothèses de collecte des données ne peuvent être évitées, car que du contraire, celles-ci se multiplient³²⁸.

Toutefois, n'est-il pas rationnel de penser que les premiers responsables et garants de leur vie privée sont en fait les personnes concernées elles-mêmes ? Ne faudrait-il pas, de prime abord, les éduquer et les responsabiliser quant à la gestion de leurs données et ce, avant de se concentrer directement sur les sanctions contre ceux qui utilisent ces mêmes données, lesquelles pouvant leur avoir été volontairement fournies³²⁹ ?

L'on insiste dès lors sur le fait que chaque individu est responsable de l'utilisation qu'il fait de ses propres données, ainsi que de la gestion de son image. En ce sens, chacun est maître des limites qu'il décide de poser entre ce qu'il souhaite garder dans sa sphère privée, ou au contraire ce qu'il ne voit pas d'inconvénient à exposer dans sa sphère publique³³⁰.

Ainsi, il nous faut placer la responsabilisation au centre des objectifs d'une législation protectrice de la vie privée et des données à caractère personnel. Il serait insensé de faire porter le poids de la responsabilité, la totalité des obligations et le contrôle des données uniquement sur ceux qui les exploitent. C'est pourquoi le RGPD doit également servir d'instrument de « *sensibilisation, d'éducation, d'information* », pour ceux qu'il aspire à protéger³³¹.

Chapitre 2. Les alternatives envisageables propres à Facebook

Il existe certaines pistes de solution, pas encore explorées par la législation, qui ont pour objectif de renforcer la protection des données des utilisateurs de Facebook. Dans ce chapitre, nous allons relever quelques-unes de ces innovations juridiques, qui pourraient s'avérer capables de révolutionner l'écosystème numérique.

³²⁸ N. RAGHENO, « Droits fondamentaux et société numérique : la vie privée existe-t-elle encore ? », *op. cit.*, p. 22.

³²⁹ *Ibid.*

³³⁰ *Ibid.*, pp. 24-25.

³³¹ *Ibid.*, p. 25.

Section 1. La possibilité de monétiser ses données

La majeure partie du profit généré par Facebook se fait via la monétisation des données à caractère personnel de ses utilisateurs, notamment au travers de la publicité. Toutefois, ceux-ci ne retirent aucune rémunération (en tout cas de manière directe) de la matière première qu'ils fournissent. Ainsi, tout internaute demeure, malgré lui, exclu de la chaîne de l'économie numérique et prisonnier du ciblage publicitaire. En définitive, la gratuité des services que lui propose Facebook cache un pillage de ses informations personnelles³³².

Par conséquent, n'est-il pas temps pour l'utilisateur de se demander si Facebook, dont les bénéfices dépassent les 7 milliards de dollars par trimestre³³³, ne devrait pas le rémunérer pour l'exploitation de ses données³³⁴ ? L'idée serait que l'individu ait à nouveau la mainmise juridique sur la propriété de ses données personnelles, car seul le droit de propriété permettrait d'assurer une maîtrise réelle de celles-ci. En outre, seule la mise en place d'un marché des data pourrait équilibrer à nouveau les relations de pouvoir entre la plateforme et ses utilisateurs, en dotant chacun d'entre eux d'un véritable capital³³⁵.

Toutefois, nous ne sommes pas d'avis qu'il s'agisse d'une solution adaptée sur le long terme car, même doublée d'une régulation performante, cet arrangement contractuel équivaldrait sans doute à une perte de contrôle encore plus alarmante des individus sur leurs données. La tentation serait trop grande pour une majorité d'individus, qui consentent déjà beaucoup trop rapidement et inconsciemment à l'utilisation de leurs données, de se faire rétribuer pour celles-ci.

C'est d'ailleurs pourquoi, dans le même ordre d'idées, le Conseil d'État rejetait explicitement cette option, s'appuyant sur l'argument que les données personnelles ne

³³² BINCTIN N., LANDREAU I., LEGER L., PELIKS G. et PEZ-PERARD V., « Résumé de l'étude », in *Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles*, (Sous la direction de LEGER L.), janvier 2018 (disponible sur <https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf>, page consultée le 3 juillet 2020), p. 8.

³³³ Le montant exact est de 7,349 milliards de dollars pour le quatrième trimestre de 2019. Voy. en ce sens M. PARK M., *Facebook Reports Fourth Quarter and Full Year 2019 Results*, 29 janvier 2020 (disponible sur : https://s21.q4cdn.com/399680738/files/doc_news/Facebook-Reports-Fourth-Quarter-and-Full-Year-2019-Results-2020.pdf, page consultée le 3 juillet 2020).

³³⁴ BINCTIN N., LANDREAU I., LEGER L., PELIKS G. et PEZ-PERARD V., « Résumé de l'étude », *op. cit.*, p. 10.

³³⁵ *Ibid.*

peuvent être monétisées au nom de la protection des libertés fondamentales ; au nom du principe de l'indisponibilité de la personne et de la non-patrimonialité du corps humain, les datas qui émanent de l'individu devraient eux aussi être exclus du marché³³⁶.

Section 2. La possibilité de payer le service, ou le « prix de la *privacy* »

Comme le souligne pertinemment J. TIROLE : « *On entend souvent dire que les plateformes devraient payer pour les données que nous leur fournissons. En pratique cependant, certaines le font effectivement, non sous la forme d'un transfert financier mais sous la forme de services non tarifés* »³³⁷. En réalité, le pacte est plutôt simple : en échange de la gratuité des réseaux sociaux, nous acceptons de confier nos données à des algorithmes qui nous offrent en retour, entre autres, des produits sur mesure grâce à la publicité ciblée³³⁸.

À l'inverse, on pourrait dès lors envisager de rendre le service proposé par Facebook payant, en contrepartie du fait que l'utilisateur ne céderait pas ses données à la plateforme. Certaines études ont d'ailleurs déjà démontré que l'internaute serait effectivement prêt à payer pour que ses données ne soient pas partagées sur la toile³³⁹. Les réflexions sont donc entamées et vont vers la mise en place d'un modèle de rétribution du citoyen pour ses données à caractère personnel³⁴⁰.

Néanmoins, nous émettons principalement deux doutes à l'encontre des deux solutions prédécrites. Premièrement, nous sommes d'avis que le mécanisme de rétribution du service ne ferait finalement qu'augmenter les recettes de Facebook, le rendant encore plus imperméable aux amendes. Deuxièmement, l'idée de payer les citoyens-consommateurs pour leurs données pourrait donner naissance à des comportements opportunistes, en ce que ces

³³⁶ CONSEIL D'ETAT, Étude annuelle 2014 : Le numérique et les droits fondamentaux, Conférence de presse du mardi 9 septembre 2014 (disponible sur <https://www.conseil-etat.fr/ressources/etudes-publications/rapports-etudes/etudes-annuelles/etude-annuelle-2014-le-numerique-et-les-droits-fondamentaux>, page consultée le 20 juillet 2020).

³³⁷ J. TIROLE, « Économie du bien commun », in *RIMHE : Revue Interdisciplinaire Management, Homme & Entreprise*, 2016/4, n° 23, Paris, PUF, 2016, pp. 101-105.

³³⁸ BINCTIN N., LANDREAU I., LEGER L., PELIKS G. et PEZ-PERARD V., « Résumé de l'étude », *op. cit.*, p. 14.

³³⁹ MBA@UNC, *The Business of Data Brokers [Infographic]*, 19 February 2015 (disponible sur <https://onlinemba.unc.edu/news/data-brokers-infographic/>, page consultée le 15 mai 2020).

³⁴⁰ LANDREAU I., LEGER L. et PEZ-PERARD V., « 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 LEGER L.), janvier 2018 (disponible sur <https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf>, page consultée le 3 juillet 2020), p. 33.

derniers pourraient être tentés de créer des identités numériques imaginaires, comme des faux profils Facebook, par appât du gain³⁴¹. De telles attitudes pourraient alors diminuer la valeur des données en rendant leur exploitation moins efficace, car basée sur des éléments falsifiés³⁴².

³⁴¹ LANDREAU I., LEGER L. et PEZ-PERARD V., « Les aspects socio-économiques et éthiques des données personnelles », *op. cit.*, p. 40.

³⁴² *Ibid.*

Conclusion

Le formidable outil qu'est Internet va malheureusement de pair avec les nombreuses dérives qu'il entraîne, lesquelles peuvent bien souvent mettre à mal les droits et libertés fondamentales du citoyen. La violation du droit à la protection des données personnelles lors des opérations de ciblage publicitaire n'en est finalement qu'un exemple parmi tant d'autres. Ce n'est un secret pour personne, le droit a tendance à se faire rattraper par la technique, et peine à suivre le rythme face à l'évolution fulgurante des médias réseaux, dont Facebook est l'un des piliers.

Le fait que la violation de la vie privée et des données à caractère personnel soit devenue quasi systématique, à tel point que plus personne ne semble s'en offusquer, ne devrait en aucun cas justifier la négligence de ne pas y mettre un terme, ou tout du moins de ne pas prendre la peine de développer des outils performants afin de l'atténuer. Que du contraire, la banalisation de la problématique devrait encore plus alarmer et pousser à réagir, mais surtout à agir.

Dans ce paysage législatif qui s'avérait quelque peu bancal, le pari ambitieux lancé par le RGPD était de moderniser le droit de la protection de la vie privée, et de manière corollaire, les données à caractère personnel. Plus qu'une simple réglementation, il était notamment question d'instaurer de nouveaux modes de fonctionnement plus respectueux des données, de redessiner les contours des obligations des responsables de traitement et des droits accordés aux individus, mais également et surtout, d'assurer une plus grande effectivité des garanties déjà offertes à l'époque de la directive 95/46.

Pari réussi ? Nous ne pouvons pas nous empêcher de rester sur la réserve. *D'un côté*, les entreprises, qui rechignent à se conformer aux nouvelles obligations, par manque de temps et/ou d'expérience³⁴³, ou parce qu'elles diabolisent le règlement et sa fonction première³⁴⁴. Force est de constater que les réseaux sociaux n'usent pas de tous les moyens qui sont en leur

³⁴³ Voy. en ce sens F. MEURICE, Head of Digital Service Design, interview réalisée par M.-E. RODRIGUEZ le 30 juillet 2020, pp. 87-89.

³⁴⁴ Voy. en ce sens F. ZÖFEL, Data Protection Officer, interview réalisée par M.-E. RODRIGUEZ le 23 juillet 2020, p. 80 : « *Les gens, et surtout les acteurs de la publicité, se représentent une loi rédigée par des avocats, pour des avocats, et dans le but de se remplir les poches sur le dos de Google. C'est tellement plus que ça. Le RGPD est la raison numéro une de la prise de conscience dans les sociétés européennes du besoin de sécuriser les systèmes d'informations* ».

pouvoir pour honorer les exigences imposées par le RGPD. Aujourd'hui, les outils mis en place par les plateformes restent clairement insuffisants : le manque de transparence flagrant dont font preuve les fournisseurs des réseaux sociaux, les paramètres de confidentialité encore et toujours configurés par défaut sur une position à risque et parfois difficilement (ou en tout cas, laborieusement) modifiables, la négligence quant au consentement du consommateur que l'on finira tout de même par noyer de publicités ciblées, ... pour ne citer qu'eux.

D'un autre côté, les utilisateurs eux-mêmes, qui révèlent allègrement aux yeux de tous des pans entiers de leur vie privée, sans prendre la pleine mesure des répercussions d'une telle exposition³⁴⁵. Peut-être est-ce l'interface des écrans et la distance inévitablement ressentie par l'individu lorsqu'il surfe sur le Web qui lui donne l'impression d'une liberté presque totale, jusqu'à lui faire éprouver un sentiment d'inaccessibilité, le mettant fictivement à l'abri de tout danger. Car c'est en fait à partir de leur navigation, de leurs recherches et de leurs *likes*, que ces derniers trahissent leur choix de consommation à des grandes entreprises multinationales. Grâce à (ou plutôt, à cause de) cette nonchalance généralisée, Facebook est devenue une mine d'or inestimable pour un bon nombre d'acteurs, au premier rang desquels se retrouvent les publicitaires³⁴⁶. Se faisant, le risque le plus important tient finalement à la perte de contrôle totale des données personnelles semées par l'internaute.

C'est pourquoi, dès aujourd'hui et plus que jamais, il est essentiel que chaque citoyen prenne activement part à la gestion de son « *identité numérique* », et qu'il participe à la limitation des atteintes susceptibles d'être portées à ses droits, mais également à ceux de ses « *amis* »³⁴⁷. Il est primordial de garder en tête qu'il existe bel et bien un commerce qui entoure les données personnelles, et il faut être conscient de la fragilité technique des réseaux sociaux à ce propos³⁴⁸.

En guise d'ultime conclusion, nous désirons mettre en lumière le fait que la thématique étudiée s'inscrit dans un paysage juridique et numérique en évolution constante, dans lequel de nombreuses améliorations restent à construire. Aujourd'hui, nous ne sommes finalement qu'aux prémices de tout ce qu'il est possible de faire³⁴⁹. La vérité appartient à

³⁴⁵ A. ARAMAZANI, « Le droit à l'oubli et internet », *op. cit.*, p. 44.

³⁴⁶ GROUPE DE TRAVAIL « ARTICLE 29 », Avis 5/2009 sur les réseaux sociaux en ligne, *op. cit.*, p. 4.

³⁴⁷ Pour reprendre le terme du réseau social Facebook.

³⁴⁸ M. SALMON et J. DESCHUYTENEER, « Introduction », *op. cit.*, pp. 8-13.

³⁴⁹ F. MEURICE, Head of Digital Service Design, interview réalisée par M.-E. RODRIGUEZ le 30 juillet 2020, p. 83

l'avenir : seule la volonté des différents acteurs, du législateur aux entreprises, en passant par les consommateurs eux-mêmes, pourra déterminer les progrès en la matière.

BIBLIOGRAPHIE

Législation

▪ *Conventions et charte*

- **Convention** de sauvegarde des Droits de l'Homme et des Libertés fondamentales, signée à Rome le 4 novembre 1950, approuvée par la loi du 13 mai 1955, *M.B.*, 19 août 1955, p. 5028, art. 8.
- **Convention** n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signée à Strasbourg le 28 janvier 1981.
- **Charte** des Droits Fondamentaux de l'Union Européenne, *J.O.U.E.*, C 326, 26 octobre 2012, p. 391, art. 8.

▪ *Règlement et directives*

- **Règlement** (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119/1, 4 mai 2016.
- **Directive** (CE) n° 95/46 du Parlement 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, 23 novembre 1995 (abrogée).
- **Directive** (CE) n° 2000/31 du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »), *J.O.U.E.*, L. 178, 17 juillet 2000.
- **Directive** (UE) n° 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de

détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *J.O.U.E.*, L. 119/89, 4 mai 2016.

▪ *Recommandation*

- **Recommandation** CM/Rec(2010)13 du Comité des ministres aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, adoptée par le Comité des ministres le 23 novembre 2010.

▪ *Proposition amendée et projet de rapport explicatif*

- **Proposition amendée** de directive du Conseil et du Parlement européen sur la protection des individus au regard du traitement de leurs données à caractère personnel, 15 octobre 1992, COM (92)422 final, p. 10.
- **CONVENTION N° 108 DU CONSEIL DE L'EUROPE**, *Projet de rapport explicatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, version du 2 juin 2016 (disponible à l'adresse suivante <https://rm.coe.int/convention-pour-la-protection-des-personnes-a-l-egard-du-traitement-au/16806b6ec3>, page consultée le 5 juillet 2020).

▪ *Code et lois*

- **Code** de droit économique, art. I.18, 6°.
- **Loi** du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur, *M.B.*, 29 août 1991 (abrogée).
- **Loi** du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, p. 5801.
- **Loi** du 6 avril 2010 relative aux pratiques du marché et à la protection du consommateur, *M.B.*, 12 avril 2010, p. 2084.
- **Loi** du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, p. 68616.

Jurisprudence

- Cour eur. D.H., arrêt *Satakunnan Markkinapörssi Oy et Satamedia Oy contre Finlande*, 27 juin 2017, req. n° 931/13, § 137.
- C.J.U.E., arrêt *Rechnungshof contre Österreichischer Rundfunk et autres*, 20 mai 2003, C-465/00, EU:C:2003:294, pt. 64.
- C.J.U.E., arrêt *Göta hovrätt contre Lindqvist*, 6 novembre 2003, C-101/01, EU:C:2003:596, pts. 24-27.
- C.J.U.E., arrêt *Republik Österreich contre Martin Huber*, 16 décembre 2008, C-524/06, EU:C:2008:724, pt. 43.
- C.J.U.E., arrêt *Tietosuojavaltuutettu contre Satakunnan Markkinapörssi Oy et Satamedia*, 16 décembre 2008, C-73/07, EU:C:2008:727, pts. 35-37.
- C.J.U.E., arrêt *College van burgemeester en wethouders van Rotterdam contre M.E.E. Rijkeboer*, 7 mai 2009, C-553/07, EU:C:2009:293, pt. 62.
- C.J.U.E., arrêt *Bonnier Audio AB e.a. contre Perfect Communication Sweden AB*, 19 avril 2012, C-461/10, EU:C:2009:293, pt. 93.
- C.J.U.E., arrêt *Google Spain SL, Google Inc. contre Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, 13 mai 2014, C-131/12, EU:C:2014:317, pts. 56-60.
- C.J.U.E., arrêt *Weltimmo s. r. o. contre Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1^{er} octobre 2015, C-230/14, EU:C:2015:639, pt. 29.
- C.J.U.E., arrêt *Peter Nowak contre Data Protection Commissioner (Irlande)*, 20 décembre 2017, C-434/16, EU:C:2017:994, pt. 34.
- C.J.U.E., arrêt *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein contre Wirtschaftsakademie Schleswig-Holstein GmbH*, 5 juin 2018, C-210/16, EU:C:2018:388.

Doctrine

- AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE, *Guide pour la prévention du profilage illicite aujourd'hui et demain*, Luxembourg, Office des publications de l'Union européenne, 2019, pp. 17-37.

- **AGENCE DES DROITS FONDAMENTAUX DE L’UNION EUROPEENNE ET CONSEIL DE L’EUROPE**, *Manuel de droit européen en matière de protection des données*, Édition 2018, Luxembourg, Office des publications de l’Union européenne, 2019, pp. 20-173.
- **ARAMAZANI A.**, « Le droit à l'oubli et internet », *R.D.T.I.*, 2011/2, n° 43, pp. 44-48.
- **BORGESIOUS F.**, “Singling out people without knowing their names: behavioural targeting, pseudonymous data, and the new Data Protection Regulation”, in *Computer Law & Security Review*, 2016, p. 259.
- **CLEMENT-FONTAINE M.**, « La plasticité de la notion de responsable de traitement », *R.A.E.*, 2018/1, pp. 36-37.
- **COUDRAY L.**, *La protection des données personnelles dans l’Union européenne : naissance et consécration d’un droit fondamental*, Sarrebruck, Éditions Universitaires Européennes, 2010, pp. 118-121.
- **CRUQUENAIRE A., DEMOULIN M., GOBERT D., LAZARO C., MARTHOZ B., MONTERO E., ROBERT R. et VAN DER PERRE A.**, « Partie 4. Se protéger des « agressions » sur Internet », in *Guide pour les utilisateurs d’Internet, rédigé par le Centre de Recherches Informatique et Droit (FUNDP – Namur) dans le cadre d’un contrat de recherches financé par le Service public fédéral Économie, P.M.E., Classes moyennes et Énergie*, (Sous la dir. de DEMOULIN M.), Bruxelles, Regis Massant, 2011, pp. 109-113.
- **CRUYSMANS E.**, « La directive 95/46/CE n’est plus, vive le R.G.P.D. ! », in *Auteurs & Media*, Vol. 2017, no. 1, p. 108.
- **CRUYSMANS E.**, « Vous gérez une page « fan » sur Facebook ? Vous êtes alors coresponsable du traitement des données personnelles », in *Les pages : obligations, contrats et responsabilités*, Vol. 2018, no. 32, p. 1.
- **DE BACKER P.**, « Préface », in *Data protection & privacy : le GDPR dans la pratique*, Limal, Anthemis, 2017, p. 11.
- **DELFORGE A.**, « Comment (ré)concilier RGPD et big data ? », *R.D.T.I.*, 2018/1, n° 70, pp. 16-20.
- **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, Larquier, 2018, pp. 375-391.
- **DE TERWANGNE C., ROSIER K. ET LOSDYCK B.**, « Le règlement européen relatif à la

protection des données à caractère personnel : quelles nouveautés ? », *J.D.E.*, 2017/8, pp. 305-313.

- **DINANT J.-M., LAZARO C., POULLET Y., LEFEVER N. ET ROUVROY A.**, *Application of Convention 108 to the profiling mechanism: Some ideas for the future work of the consultative committee (T-PD)*, Strasbourg, Doc. T-PD(2008)01, 2008, pp. 3-11.
- **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. 128-129.
- **FRANCQ S.**, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, Bruxelles, Bruylant, 2005, p. 8.
- **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, p. 476.
- **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. 277-307.
- **JACQUEMIN H.**, « Le big data à l'épreuve des pratiques du marché et de la protection du consommateur », *R.D.T.I.*, n° 70/2018, p. 79.
- **LEVIN A. ET SANCHEZ ABRIL P.**, "Two Notions of Privacy Online", in *Vanderbilt J. of Ent. And Tech. Law*, 2009, p. 1017.
- **METOU A.**, « Vous avez dit "spyware" ? », in *Technologies Internationales*, n° 86, juillet-août 2002, p. 34.
- **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. 53-68.
- **MOINY J.-P.**, « Facebook au regard des règles européennes concernant la protection des données », *R.E.D.C.*, 2010/2, pp. 236-243.
- **MOINY J.-P. et POULLET Y.**, « Les réseaux sociaux, le droit et les volontés qui les animent », in *Social Media : le droit ou l'anarchie ? / Social Media : recht of anarchie*, Bruxelles, Bruylant, 2012, pp. 7-9.
- **PHILIPPART DE FOY A. et VAN GOSSUM K.**, « Les cookies : état des lieux et perspectives », *R.D.T.I.*, n° 52/2013, p. 6.
- **PONSART C. ET ROBERT R.**, « Le règlement européen de protection des données personnelles », *J.T.*, 2018, pp. 422-425.

- **POULLET Y.**, « Consentement et RGPD : des zones d’ombre ! », *D.C.C.R.*, 2019/1-2, n° 122-123, pp. 6-18.
- **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, p. 41.
- **RAGHENO N.**, « Droits fondamentaux et société numérique : la vie privée existe-t-elle encore ? », in *Data protection & privacy : le GDPR dans la pratique*, Limal, Anthemis, 2017, pp. 18-25.
- **RAGHENO N. ET LAMBRECHT P.**, « Avant-propos », in *Data protection & privacy : le GDPR dans la pratique*, Limal, Anthemis, 2017, p. 15.
- **RANSE S.**, « Le *profiling* des internautes au regard du droit au respect de la vie privée : le coût de l’efficacité ! », *R.D.T.I.*, n° 20/2004, pp. 39-41.
- **SALMON M. et DESCHUYTENEER J.**, « Introduction », in *Les réseaux sociaux et le droit*, Bruxelles, Éditions Larcier, 2014, pp. 8-13.
- **SOMERS G.**, “Can Confidentiality be upheld in the Information Society?”, *R.E.D.C.*, 2011/3, p. 531.
- **TINIERE R.**, « Article 8. - Protection des données à caractère personnel », in *Charte des droits fondamentaux de l’Union européenne*, Bruxelles, Bruylant, 2017, p. 214.
- **TIROLE J.**, « Économie du bien commun », in *RIMHE : Revue Interdisciplinaire Management, Homme & Entreprise*, 2016/4, n° 23, Paris, PUF, 2016, pp. 101-105.
- **TUFFERY S.**, *Data mining et statistique décisionnelle. L’intelligence dans les bases de données*, Paris, Éd. Technip, 2005, p. VII.
- **VAN GOSSUM K.**, *Het Internet en de verwerking van persoonsgegevens door lokale besturen: algemeen overzicht en praktische toepassingen*, Brugge, Vanden Broele, 2012, p. 68.
- **VOGEL L. ET VOGEL J.**, « I. - Publicité sur Internet » in *Traité de droit économique – Tome 3 : Droit de la consommation*, Bruxelles, Bruylant, 2017, pp. 161-170.

Autres

▪ *Articles en ligne*

- **BAMDE A.**, *Le Droit dans tous ses états - RGPD : les concepts de privacy by design et de privacy by default*, 22 décembre 2018 (disponible sur

- <https://aurelienbamde.com/2018/12/22/rgpd-les-concepts-de-privacy-by-design-et-de-privacy-by-default/>, page consultée le 05 juillet 2020).
- 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 LEGER L.), janvier 2018 (disponible sur <https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf>, page consultée le 06 août 2020), pp. 77-82.
 - BINCTIN N., LANDREAU I., LEGER L., PELIKS G. et PEZ-PERARD V., « Résumé de l'étude », in *Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles*, (Sous la direction de LEGER L.), janvier 2018 (disponible sur <https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf>, page consultée le 3 juillet 2020), p. 8.
 - BYGRAVE L. A., *Minding the machine: article 15 of the EC Data Protection Directive and automated profiling* (disponible sur <http://classic.austlii.edu.au/au/journals/PrivLawPRpr/2000/40.html>, page consultée le 20 mai 2020).
 - CONFOLANT A., *Licence perpétuelle des données : Facebook fait volte-face*, 18 février 2009 (disponible sur <https://www.itespresso.fr/licence-perpetuelle-des-donnees-facebook-fait-volte-face-24411.html>, page consultée le 10 novembre 2019).
 - DEGREEF V., *La maîtrise du soi multiple face à l'exhibitionnisme identitaire. L'identité en termes de contrôle et d'autonomie au travers des logiciels sociaux*, Série des Working Papers du Centre Perelman de philosophie du droit n° 2008/4, Année académique 2007-2008, (disponible sur <https://www.philodroit.be/La-maitrise-du-soi-multiple-face-a?lang=fr>, page consultée le 20 avril 2020).
 - DINANT J.-M., LAZARO C., POULLET Y., LEFEVER N. ET ROUVROY A., *L'application de la Convention 108 au mécanisme de profilage : Éléments de réflexion destinés au travail du futur Comité consultatif (T-PD)*, 11 janvier 2008 (disponible sur <https://www.coe.int/fr/web/data-protection/reports-studies-and-opinions>, page consultée le 15 mai 2020), pp. 3-14.
 - JANSSEN D., *Le dark web : Qu'est-ce que c'est exactement et que pouvez-vous y trouver ?*, 28 avril 2020 (disponible sur

- <https://vpnoverview.com/fr/confidentialite/navigation-anonyme/le-dark-web/>, page consultée le 10 juillet 2020).
- JOURNAL DU NET, *Nombre d'utilisateurs de Facebook dans le monde*, 31 juillet 2020 (disponible sur <https://www.journaldunet.com/ebusiness/le-net/1125265-nombre-d-utilisateurs-de-facebook-dans-le-monde/>, page consultée le 8 août 2020)
 - LA DERNIERE HEURE, *Facebook rassure ses utilisateurs*, 17 février 2009 (disponible sur <https://www.dhnet.be/actu/new-tech/facebook-rassure-ses-utilisateurs-51b7b33fe4b0de6db9889213>, page consultée le 11 novembre 2019).
 - LANDREAU I., LEGER L. et PEZ-PERARD V., « 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 LEGER L.), janvier 2018 (disponible sur <https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf>, page consultée le 3 juillet 2020), pp. 33-40.
 - LANDREAU I. et SFADJ R., « Le RGPD, un pas dans la bonne direction ? », in *Rapport de Génération Libre, Mes data sont à moi, Pour une patrimonialité des données personnelles*, (Sous la direction de LEGER L.), janvier 2018 (disponible sur <https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf>, page consultée le 6 août 2020), p. 77.
 - MBA@UNC, *The Business of Data Brokers [Infographic]*, 19 February 2015 (disponible sur <https://onlinemba.unc.edu/news/data-brokers-infographic/>, page consultée le 15 mai 2020).
 - MR MONDIALISATION, *De Google à Facebook : « si c'est gratuit, vous êtes le produit »*, 7 mai 2016 (disponible sur <https://mrmondialisation.org/google-facebook-gratuit-vous-etes-produit/>, page consultée le 8 août 2020).
 - PARK M., *Facebook Reports Fourth Quarter and Full Year 2019 Results*, 29 janvier 2020 (disponible sur : https://s21.q4cdn.com/399680738/files/doc_news/Facebook-Reports-Fourth-Quarter-and-Full-Year-2019-Results-2020.pdf, page consultée le 3 juillet 2020).
 - ROBILLART O., *Documents personnels : Facebook renonce à la licence perpétuelle*, 18 février 2009 (disponible sur <https://www.silicon.fr/documents-personnels->

- [facebook-renonce-a-la-licence-perpetuelle-34112.html](https://dokodoc.com/queue/le-profilage-des-individus-a-l-heure-du-cyberespace-un-defi-.html), page consultée le 11 novembre 2019).
- **WALTER J.-P.**, *Le profilage des individus à l'heure du cyberspace : un défi pour le respect du droit à la protection des données*, 2009 (disponible sur <https://dokodoc.com/queue/le-profilage-des-individus-a-l-heure-du-cyberespace-un-defi-.html>, page consultée le 10 juillet 2020), pp. 2-17.
 - **X.**, *Fiche d'entreprise de Facebook Ireland* (disponible sur <https://www.societe.com/societe/facebook-ireland-limited-814665519.html>, page consultée le 15 juillet 2020).
- *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, page consultée le 10 juillet 2020).
 - **Facebook**, *À propos* (disponible sur https://www.facebook.com/pg/facebook/about/?ref=page_internal, page consultée le 8 août 2020).
 - **Facebook**, *Paramètres et outils de confidentialité – Votre activité et Comment les autres peuvent vous trouver et vous contacter* (disponible sur : <https://www.facebook.com/settings?tab=privacy>, page consultée le 5 juillet 2020).
 - **Facebook**, *Politique d'utilisation des données* (disponible sur <https://www.facebook.com/privacy/explanation>, page consultée le 20 juillet 2020).
 - **Facebook**, *Propriété intellectuelle* (disponible sur https://www.facebook.com/help/intellectual_property, page consultée le 20 juillet 2020).
 - **Facebook Business**, *Qu'est-ce que le Règlement général sur la protection des données (RGPD) ?* (disponible sur <https://www.facebook.com/business/gdpr>, page consultée le 12 juillet 2020).
 - **Facebook Newsroom**, *Facebook to Establish International Headquarters in Dublin Ireland*, le 2 octobre 2008 (disponible sur <https://newsroom.fb.com/news/2008/10/facebook-to-establish-international->

[headquarters-in- dublin-ireland/](#), page consultée le 15 juillet 2020).

■ *Publications officielles*

- **COMITE CONSULTATIF DE LA « CONVENTION 108 »**, Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées, T-PD(2017)01, 23 janvier 2017, § 6.2.
- **COMMISSION DE LA PROTECTION DE LA VIE PRIVEE**, Avis 29/2007 relatif aux nouveaux modes de consommation médiatique et à la protection de la vie privée, 19 septembre 2007, p. 6, point 32.
- **COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES (CNIL)**, *La publicité ciblée en ligne, communication présentée en séance plénière*, 5 février 2009 (disponible sur
http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/Publicite_Ciblee_rapport_VD.pdf, page consultée le 5 juillet 2020), pp. 5-11.
- **CONSEIL D'ETAT**, Étude annuelle 2014 : Le numérique et les droits fondamentaux, Conférence de presse du mardi 9 septembre 2014 (disponible sur <https://www.conseil-etat.fr/ressources/etudes-publications/rapports-etudes/etudes-annuelles/etude-annuelle-2014-le-numerique-et-les-droits-fondamentaux>, page
consultée le 20 juillet 2020).
- **GROUPE DE TRAVAIL « ARTICLE 29 »**, Avis 4/2007 sur le concept de données à caractère personnel, WP 136, (01248/07/FR), 20 juin 2007, pp. 6-13.
- **GROUPE DE TRAVAIL « ARTICLE 29 »**, Avis 5/2009 sur les réseaux sociaux en ligne, WP 163, 12 juin 2009, (01189/09/FR), pp. 4-5.
- **GROUPE DE TRAVAIL « ARTICLE 29 »**, Avis 1/2010 sur les notions de responsable du traitement et de sous-traitant, WP 169, 16 février 2010, (00264/10/FR), pp. 4-14.
- **GROUPE DE TRAVAIL « ARTICLE 29 »**, Avis 2/2010 sur la publicité comportementale en ligne, WP 171, 22 juin 2010, (00909/10/FR), p. 5.
- **GROUPE DE TRAVAIL « ARTICLE 29 »**, Avis 3/2010 sur le principe de responsabilité, WP 173, 13 juillet 2010, (00062/10/FR), p. 2.
- **GROUPE DE TRAVAIL « ARTICLE 29 »**, Avis 8/2010 sur le droit applicable, WP 179, 16 décembre 2010, (0836-02/10/FR), p. 2.

- **GROUPE DE TRAVAIL « ARTICLE 29 »**, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, WP 217, 9 avril 2014, (844/14/FR), pp. 26-28.
- **GROUPE DE TRAVAIL « ARTICLE 29 »**, Avis 05/2014 sur les techniques d'anonymisation, WP 216, 10 avril 2014, (0829/14/FR), p. 3.
- **GROUPE DE TRAVAIL « ARTICLE 29 »**, Lignes directrices 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), pp. 4-18.
- **GROUPE DE TRAVAIL « ARTICLE 29 »**, Lignes directrices sur la transparence au sens du règlement (UE) 2016/679, WP 260 rév.01, adoptées le 29 novembre 2017 et révisées le 11 avril 2018, (17/FR), p. 6.
- **WORKING PARTY « ARTICLE 29 »**, Opinion 03/2013 on purpose limitation, WP 203, 2 April 2013, (00569/13/EN), p. 12.
- **WORKING PARTY « ARTICLE 29 »**, Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain, WP 179 update, 16 décembre 2015 (176/16/EN), p. 8.

▪ *Sites Internet*

- ***Internet sans crainte*** : un programme national et européen (disponible sur <https://www.internetsanscrainte.fr/projet>, page consultée le 19 novembre 2019).
- ***Adblock Plus*** : surfez sur Internet sans publicités agaçantes (disponible sur <https://adblockplus.org/>, page consultée le 19 novembre 2019).

ANNEXES. Retranscription des interviews

Interview n° 1. François Zöfel, Data Protection Officer – 23 juillet 2020

Animatrice : Bonjour Monsieur, je vous remercie d’avoir répondu favorablement à mon invitation. Je suis ravie d’avoir l’opportunité de vous interviewer dans le cadre de mon mémoire sur la protection des données à caractère personnel au regard de la publicité ciblée. Je me présente brièvement, je m’appelle Marie-Emmanuelle Rodriguez, j’ai 25 ans et je suis étudiante en dernière année de Master en Droit à l’UCL. Je propose que vous vous présentiez à votre tour, afin que nous puissions faire plus ample connaissance.

Intervenant : Bonjour Mademoiselle, je m’appelle François Zöfel, j’exerce la profession de Data Protection Officer au sein de la société Approach Belgium, dans laquelle je travaille depuis maintenant plus de deux ans. Il s’agit d’une société spécialisée en cyber-sécurité, avec plus de soixante-cinq consultants qui œuvrent notamment dans les domaines de « *Cyber Resilience* », de « *Governance, Risk & Compliance* » et de « *Digital Identity & Trust* ». À l’époque, j’ai suivi des études à l’EICW, l’École Industrielle et Commerciale de Wavre, à l’ULB et enfin à Solvay, où j’ai terminé mon parcours avec une année supplémentaire en « *Executive Master in IT Management* ».

A : Parfait, je suis enchantée de faire votre connaissance. Aujourd’hui, l’objet de notre entretien concerne la protection des données à caractère personnel, et le défi que représente la publicité ciblée pour celle-ci, et plus particulièrement sur les réseaux sociaux tels que Facebook. Mon but est d’en apprendre davantage sur vos opinions quant à la publicité que l’on peut rencontrer actuellement sur Internet. Par conséquent, sentez-vous libre de vous exprimer sans filtre, et n’hésitez pas à étoffer vos réponses en détaillant vos propos.

Si vous me le permettez, je tiens à enregistrer notre rencontre afin de pouvoir retranscrire et analyser toutes les informations par la suite.

Si cela vous convient, cet entretien devrait durer une vingtaine de minutes. Avez-vous des questions jusqu’à présent ?

I : Non, tout est parfait, merci.

A : La première question que j'aimerais vous poser est : *que répondriez-vous aux utilisateurs de Facebook qui déclarent à propos de la protection de leurs données à caractère personnel : je n'ai rien à cacher, pourquoi m'en préoccuper ?*

I : C'est un long débat, c'est d'ailleurs une réflexion que l'on nous fait souvent dans le cadre de notre métier. Généralement, je m'appuie sur des exemples historiques, comme l'utilisation de machines IBM par les nazis pour compter les juifs. La plupart du temps, les gens qui estiment ne rien avoir à cacher se targuent d'un cadre moral très strict : ils sont chrétiens ou conservateurs, « boomers », et assez conventionnels. Si ces personnes-là n'ont pas peur d'être exposées, c'est parce qu'elles ne sont jamais sorties du cadre bien classique de leur milieu et n'ont jamais été moquées et/ou persécutées. Ces individus ne sont pas homosexuels, ou handicapés, ou de couleur, ou d'une autre religion que le christianisme. Dès lors, ils se montrent confiants parce que les propriétaires de Facebook sont comme eux : hétérosexuels, blancs et chrétiens.

Il m'arrive donc de retourner la situation et de leur proposer d'imaginer que l'Arabie Saoudite rachète Facebook et commence à cataloguer tous les gens qui mangent du porc en étudiant leurs photos Instagram et leurs recettes partagées... Souvent, ce discours fait son petit effet ! Toutefois, il reste que c'est un sujet assez sensible, même si je peux facilement me permettre de jouer sur le terrain des croyances, étant donné que je suis athée. En bref, je dirais qu'il est intéressant de retourner le cadre moral et de demander aux gens comment ils le vivraient.

A : Merci pour cette réponse très intéressante, qui m'apporte un point de vue neuf sur la situation. La deuxième question à propos de laquelle il m'intéresserait de connaître votre avis est la suivante : *quel serait selon vous le moyen le plus percutant de conscientiser les gens afin qu'ils veillent à la protection de leurs données personnelles ?*

I : Souvent, ce qui fonctionne le mieux est de montrer aux internautes ce que l'on sait déjà d'eux. Les gens ne se rendent pas compte de l'étendue des données collectées, mais une fois que l'on commence à parler à un inconnu du nom de ses enfants ou de sa pointure de chaussures, la prise de conscience est quasi instantanée.

A : La troisième question que j'aimerais vous poser est celle-ci : *quelle est selon vous la plus grande lacune en termes de protection des données à ce jour ?*

I : La plus grande lacune, c'est difficile de choisir... À mon sens, c'est extrêmement dommage que si peu de gens comprennent le RGPD. C'est pourtant une loi très simple à lire, qui a vraiment été pensée pour le citoyen. Les gens, et surtout les acteurs de la publicité, se représentent une loi rédigée par des avocats, pour des avocats, et dans le but de se remplir les poches sur le dos de Google. C'est tellement plus que ça. Le RGPD est la raison numéro une de la prise de conscience dans les sociétés européennes du besoin de sécuriser les systèmes d'informations.

Je suis d'avis que les transferts de données entre entités posent également question. En effet, le « *monde technologique* » moderne est un écosystème de micro-services. La moindre application utile et légitime, pour réserver un restaurant ou un taxi, fonctionne en utilisant des « *briques* » technologiques fournies par d'autres sociétés technologiques : les données sont hébergées sur Amazon, l'application utilise des gifs qui proviennent de Facebook, les API pour les développeurs sont présentées par encore une autre société qui elle, héberge ses données chez Microsoft, etc. En résumé, chaque startup partage votre email avec au moins cinq ou six acteurs Cloud différents, tous étrangers et la plupart extra-européens, pour des raisons qui sont valides techniquement. Toutefois, c'est impossible à gérer correctement, et encore moins à expliquer aux utilisateurs.

A : Suite à votre réponse à la question précédente : *quelle pourrait être une piste de solution à apporter ?*

I : Pour ce qui est de la compréhension de la loi, je dirais qu'il faut à tout prix miser sur l'éducation, l'éducation, et encore l'éducation des citoyens. Il faut comprendre l'Europe et son fonctionnement, mais également les raisons pour lesquelles la loi informatique et libertés est apparue en France dans les années 1978, par exemple. En bref, il est vraiment nécessaire d'étudier l'Histoire.

Pour ce qui est des transferts, je n'ai pas de solution, mais je pense qu'il serait tout à fait envisageable d'automatiser la cartographie des entités qui traitent les données à caractère

personnel. Si au lieu de devoir lire des pages et des pages de *privacy policy* (en règle générale assez indigestes qui plus est), il était possible d'avoir accès à une carte du monde avec dans chaque pays, les informations collectées et le logo de la société en question, ce serait déjà beaucoup plus clair pour tout le monde.

A : Enfin, la dernière question sur laquelle j'aimerais me pencher est la suivante : *au cours de l'exercice de votre profession, avez-vous déjà eu un client réclamant plus de protection pour ses données dans le contexte de la publicité ciblée (sur les réseaux sociaux ou de manière plus large) ?*

I : J'ai beaucoup travaillé avec des publicitaires, donc c'était plutôt des gens qui ne comprenaient pas pourquoi on voulait protéger les données à caractère personnel. Je ne travaille pas avec des particuliers, mais j'ai tout de même souvent l'occasion d'expliquer à mon entourage qu'il est important d'utiliser les modes anonymes des browsers et de changer de browser entre son travail, sa banque, etc. (par exemple, utiliser Google chrome pour son boulot, Firefox pour sa banque, et Edge pour l'e-commerce).

Je ne sais pas si cela va dans le sens de la question, mais je peux citer l'exemple du New York Times qui, à l'arrivée du RGPD, a décidé de ne plus faire de tracking en Europe, car leur lectorat européen était trop peu étendu que pour investir dans la conformité du RGPD, mais trop étendu que pour être ignoré complètement. Grâce à cette décision d'arrêter la publicité ciblée, leurs revenus ont finalement augmenté...

A : D'accord Monsieur, merci pour toutes ces précieuses pistes de réflexion, je trouve votre point de vue très intéressant, il m'apporte des éléments dont je n'avais pas forcément conscience auparavant. Encore merci d'avoir pris le temps de répondre à mes différentes questions, les réponses seront utilisées à bon escient. Je vous souhaite un bel été !

I : C'était avec plaisir Mademoiselle, si vous avez d'autres questions, surtout n'hésitez pas. À bientôt !

Interview n° 2. Frédérique Meurice, Head of Digital Service Design – 30 juillet 2020

Animatrice : Bonjour Madame, je vous remercie d’avoir répondu favorablement à mon invitation. Je suis ravie d’avoir l’opportunité de vous interviewer dans le cadre de mon mémoire sur la protection des données à caractère personnel au regard de la publicité ciblée. Je me présente brièvement, je m’appelle Marie-Emmanuelle Rodriguez, j’ai 25 ans et je suis étudiante en dernière année de Master en Droit à l’UCL. Je propose que vous vous présentiez à votre tour, afin que nous puissions faire plus ample connaissance.

Intervenante : Bonjour, je m’appelle Frédérique Meurice, je suis actuellement Responsable de la conception des services numériques chez Voo, ou en anglais « *Head of Digital Service Design* », et ce depuis maintenant presque 2 ans. Auparavant, j’ai notamment travaillé chez Partenamut en tant que « *Digital Channel Manager* », ainsi que pour une banque privée, toujours dans la branche digitale. Je suis diplômée de l’ESCIP School of International Business, et au début de ma carrière, j’ai pas mal voyagé pour apprendre les langues mais également pour avoir l’opportunité de travailler dans des environnements différents, que ce soit au Mexique, au Royaume-Uni, en Espagne, ou encore en France.

A : Parfait, je suis enchantée de faire votre connaissance, et d’en apprendre plus sur votre parcours qui me semble très riche. Aujourd’hui, l’objet de notre entretien concerne la protection des données à caractère personnel, et le défi que représente la publicité ciblée pour celle-ci, et plus particulièrement sur les réseaux sociaux tels que Facebook. Mon but est d’en apprendre davantage sur vos opinions quant à la publicité que l’on peut rencontrer actuellement sur Internet. Par conséquent, sentez-vous libre de vous exprimer sans filtre, et n’hésitez pas à étoffer vos réponses en détaillant vos propos.

Si vous me le permettez, je tiens à enregistrer notre rencontre afin de pouvoir retranscrire et analyser toutes les informations par la suite.

Si cela vous convient, cet entretien devrait durer une petite heure. Avez-vous des questions jusqu’à présent ?

I : Tout est parfaitement clair, merci. Je voudrais juste préciser d'emblée qu'il y a énormément de choses à dire sur la thématique, c'est pourquoi il est parfois compliqué de structurer sa pensée. Que ce soit d'un point de vue marketing, technique, étatique ou même d'un point de vue utilisateur, il s'agit d'un sujet qui peut être abordé sous de nombreux angles différents, alors qu'aujourd'hui, nous ne sommes qu'aux prémices de tout ce qu'il est possible de faire. Malheureusement, les gens, et les entreprises elles-mêmes, n'ont pas encore tout à fait conscience des dangers.

A : D'accord, merci pour cette précision. La première question que j'aimerais vous poser est : *que répondriez-vous aux utilisateurs de Facebook qui déclarent à propos de la protection de leurs données à caractère personnel : je n'ai rien à cacher, pourquoi m'en préoccuper ?*

I : Il faut considérer la thématique comme un iceberg, dont la plupart des gens ne vont voir que la face émergée. On pourrait dire qu'il y a encore deux couches en-dessous : la couche où les entreprises opèrent pour faire transiter les données, pour offrir une superbe expérience, ou alors pour offrir des informations qui sont très importantes pour l'internaute (dans ce cas-ci, on vise typiquement les banques) et la couche qui se situe encore en-dessous, à savoir le « *dark web* »³⁵⁰. Globalement, il faut se rendre compte qu'il s'agit d'une sorte de marché noir de la donnée à caractère personnel, c'est-à-dire que l'on peut vendre une identité complète, des numéros de cartes bancaires, ... En fait, on va vendre les données d'une vie.

Les gens n'ont pas compris que Facebook devient une arme de destruction massive en devenir. Pourquoi ? Parce qu'en fait, derrière Facebook, il y a des millions d'algorithmes et d'intelligences artificielles qui manipulent toutes les données et qui recalculent ces dernières, quasiment de manière systématique et constante, afin de proposer du contenu aux internautes.

Je ne sais pas si tu as entendu parler du scandale Cambridge Analytica ?

A : Oui, bien sûr !

³⁵⁰ Également connu sous le nom d'« *Internet clandestin* » ou d'« *Internet sombre* », le dark web est généralement présenté comme la partie « cachée » et dangereuse d'Internet, car non réglementée. Complexe à atteindre, il est fréquemment associé à des pratiques illégales telles que le marché noir de drogues et d'armes ou les vidéos à caractère pédopornographique. Voy. en ce sens D. JANSSEN, *Le dark web : Qu'est-ce que c'est exactement et que pouvez-vous y trouver ?*, 28 avril 2020 (disponible sur <https://vpnoverview.com/fr/confidentialite/navigation-anonyme/le-dark-web/>, page consultée le 10 juillet 2020).

I : Ce n'est rien d'autre qu'une arme de destruction massive, parce que finalement, c'est la preuve qu'ils ont été capables de faire de la propagande à grande échelle pour arriver à leurs fins. Au début, il est vrai que c'était peut-être de manière innocente, Facebook n'était qu'un simple réseau pour entretenir des relations avec les étudiants. Mais aujourd'hui, c'est réellement une arme de destruction massive en devenir. Si les gens ne prennent pas conscience de ce qu'il se passe d'une part, pour la protection de leurs données, et d'autre part, pour tout le contenu qui y transite, on risque de tomber dans des circuits infernaux.

Par conséquent, il y a la couche du dark web, où l'on utilise tout ce que l'internaute dépose sur la toile, pas pour lui voler sa vie, mais pour la vendre ! Pour l'autre couche, il faudrait dire à l'internaute « *oui, tu n'as peut-être rien à cacher, mais il faut que tu saches que tu exposes des choses, mais ces choses-là, une entreprise comme Facebook va les prendre et les manipuler pour te suggérer autre chose* ». Si c'était uniquement pour être en vase clos, il n'y aurait pas de problème. Sauf qu'aujourd'hui, il est très compliqué pour un utilisateur lambda d'aller bloquer tous ses paramètres pour être sûr de ne communiquer qu'avec ses amis ou sa famille. En fait, j'ai vérifié et lorsque Facebook a été lancé (pour ma part j'y suis inscrite depuis 2007), il était facile de créer des groupes d'utilisateurs et de cacher tout son contenu. J'acceptais quelqu'un et systématiquement, Facebook me proposait de le mettre dans une catégorie, comme par exemple la catégorie des gens avec lesquels je désire uniquement partager ma photo de profil, mon nom et mon prénom.

A : Oh, je ne savais pas vraiment qu'à l'époque Facebook avait mis ce système en place...

I : Ah si, on pouvait le faire, et c'était beaucoup plus facile qu'aujourd'hui ! Maintenant, je me suis dit « *tiens, je vais chercher comment faire* », et en fait, c'est vraiment fastidieux, c'est devenu tellement compliqué... Finalement, au fur et à mesure que le temps passe, une fois que tu as mis le doigt dans l'engrenage, bon courage pour cacher tout ça.

Pour revenir à ta question, je parlerais donc aux utilisateurs du dark web, car peu d'entre eux ont conscience de la menace qu'il représente, et je jouerais également sur le fait que Facebook va analyser les données à caractère personnel que l'internaute partage pour pouvoir ensuite lui proposer quelque chose de bien précis.

A : On peut donc parler de manipulation ?

I : C'est de la manipulation, exactement ! C'est quand même assez dangereux.

A : Effectivement... La deuxième question à propos de laquelle il m'intéresserait de connaître votre avis est la suivante : *quel serait selon vous le moyen le plus percutant de conscientiser les gens afin qu'ils veillent à la protection de leurs données personnelles ?*

I : Je ferais la même chose que la sécurité routière qui, par des vidéos choquantes, éduque les gens. En Suisse, ils sont très forts là-dedans, ils publient des vidéos où tu es complètement bluffé. Selon moi, c'est vraiment le rôle de l'État, du législateur et des entreprises de lancer ce genre de campagnes là. J'ai l'impression qu'aujourd'hui, il n'y a pas vraiment de lobbyistes pour la protection des données personnelles. Il y a également trop peu de reportages qui sont intéressants, bien faits et surtout accessibles, parce qu'on ne va pas se le cacher, il y a quand même une partie de la population qui ne comprend pas...

A : Sur ce point je vous rejoins complètement, c'est vraiment un sujet complexe qui mériterait que l'on s'y attarde, mais il faut que les gens disposent des bons outils pour le comprendre.

I : Par exemple, l'application TikTok... Au-delà de la santé mentale des gens (parce que l'on crée une addiction, mais ça c'est encore une autre histoire), le fait qu'il y ait autant d'utilisateurs européens qui créent leur compte via Facebook, alors que c'est une application chinoise, ce n'est pas anodin ! Toutefois, ça reste très compliqué de faire comprendre les impacts et les enjeux de tout ça au grand public. Par conséquent, je pense que tout ce qui est vidéos et reportages, c'est un bon outil. C'est vraiment par l'éducation et la conscientisation que l'on va arriver à faire comprendre aux gens ce qu'il se passe.

D'un point de vue métier, j'aurais dit que lorsque l'on fait des interfaces en design, on insère par exemple des petits messages grâce au « I » pour solliciter l'attention des internautes, ou lors de la création d'un compte avec mot de passe, on requiert qu'il y ait au moins une majuscule, des chiffres, etc. Toutefois, il faut se mettre à la place du client, qui a besoin de créer son compte parce qu'il veut faire quelque chose, et là on vient lui mettre une barrière qui complique tout. Sauf qu'à ce moment-là, l'internaute n'est pas dans l'optique de comprendre pourquoi la sécurité est importante, il est plutôt dans l'optique d'acheter quelque

chose, de remplir un dossier, etc. En fait, ce n'est pas le bon moment ! Le problème n'est pas de créer des interfaces avec des warnings, mais plutôt d'éduquer les gens au préalable.

A : Encore une fois, je rejoins votre avis. La troisième question que j'aimerais désormais vous poser est celle-ci : *quelle est selon vous la plus grande lacune en termes de protection des données à ce jour ?*

I : D'après moi, il y a trois choses. Premièrement, il s'agit vraiment du niveau d'alerte des gens, qui n'est pas là. Le manque de conscientisation de la population est une catastrophe. On dit souvent que la majeure partie des problèmes en « IT »³⁵¹ se situent entre le clavier et la chaise. De toute façon, on ne va rien pouvoir faire pour la bêtise humaine, mais on peut aider à éduquer.

Deuxièmement, il y a les aspects techniques. Quand une entreprise veut créer un site Web ou une application, elle va construire une sorte d'architecture. C'est à ce moment-là que l'entreprise commence à bâtir les fondations, pour être sûre que tout fonctionne. Aujourd'hui, les entreprises ne sont pas ou très peu conscientisées des risques qu'elles prennent lorsqu'elles construisent les architectures des sites Web ou des applications en question. J'ai pris conscience de la problématique lorsque je travaillais pour une banque privée, où lors des réunions pour la construction de l'architecture, on est un peu dans une ambiance de guerre. On utilise des termes militaires pour définir les couches de protection d'une architecture en banque, car il s'agit de sécurité ! Néanmoins, quand je suis arrivée dans d'autres boîtes, le manque se faisait sentir.

Les entreprises doivent réellement trouver le moyen de sécuriser les données tout en offrant à l'utilisateur la meilleure expérience possible. Le problème c'est que les entreprises n'ont pas conscience de ça, pour elles, sécuriser veut dire que l'on va mettre en danger l'expérience utilisateur, alors que ce n'est pas vrai du tout ! Aujourd'hui, on est complètement capable de créer une expérience utilisateur magnifique, tout en proposant une solution hyper sécurisée. Ce qui est intéressant, c'est de regarder comment les banques ont évolué par rapport à ça, même au niveau des impôts. Je ne sais pas si tu as déjà entendu parler de « *itsme* » ?

³⁵¹ Les « *Information Technology* » en anglais et « *Technologies de l'information et de la communication* » (TIC) en français désignent les techniques utilisées dans le traitement et la transmission des informations.

A : Oui bien sûr, c'est une l'application qui permet de se connecter, de partager ses données d'identité et de signer avec son smartphone.

I : Voilà, c'est très facile à utiliser. Si on devait transposer cet exemple-là dans la vie physique, c'est comme si tu avais un coffre-fort, dont tu es la seule à avoir la clé. Le moment où tu tournes ta clé dans la serrure pour ouvrir le coffre-fort, c'est « *itsme* ».

Pour revenir à la question, il y a effectivement le manque de conscientisation des gens, mais également les aspects techniques. Il est important de structurer correctement les IPA, c'est-à-dire toutes les espèces de micro-briques qui rassemblent toutes les données, et qui les diffusent à droite et à gauche dans l'application. C'est à ce moment-là qu'il faut déjà penser à la sécurité.

Dans l'entreprise, le fait d'avoir instauré un régulateur en interne, le Data Protection Officer, ce n'est pas suffisant, car il est généralement tout seul dans son bureau. Selon moi, il devrait être accompagné du personnel qui gère l'architecture business et technique. La troisième lacune n'est finalement que celle-ci : on minimise le rôle du DPO. J'espère que ce n'est pas une généralité dans toutes les boîtes, mais on peut tomber sur des gens qui n'ont pas conscience de ce qu'est une architecture IT et de ce qui peut être exposé. D'après moi, le DPO idéal est quelqu'un qui a étudié le droit de la protection des données, et qui est capable de lire une architecture IT. En fait, le DPO ne doit pas se retrouver tout seul au légal, mais être un électron libre entre tout ce qui est architecture, business et légal. Le problème est qu'aujourd'hui, il a du mal à trouver sa place dans beaucoup d'entreprises, parce qu'il est vu comme un agent de police avec un sifflet, alors que pas du tout ! Il s'agit simplement de quelqu'un qui doit aider à la co-construction d'un environnement. Il faut repenser la fonction.

A : Une autre question sur laquelle j'aimerais me pencher est celle-ci : *au cours de l'exercice de votre profession, avez-vous déjà eu un client réclamant plus de protection pour ses données dans le contexte de la publicité ciblée (sur les réseaux sociaux ou de manière plus large) ?*

I : Jamais. Toutefois, il y a deux choses : lorsqu'il a fallu modifier les *cookies policies* suite à la nouvelle réglementation du GDPR, un utilisateur avait l'opportunité d'envoyer une demande à une entreprise, et recevoir dans un délai de 72 heures, l'intégralité des

informations que l'entreprise possédait à son sujet. En tant qu'utilisateur, on peut donc contacter par exemple Proximus, notre banque, notre assurance, en demandant toutes les informations qu'ils ont sur nous.

A : Il s'agit vraiment d'une obligation ?

I : Oui, c'est une obligation. En réalité, c'est même assez contraignant voir même impossible de réunir toutes les informations demandées en 72 heures. Toutefois, il faut savoir qu'à l'époque, les entreprises ont eu moins d'un an pour mettre en place la nouvelle réglementation RGPD, ce qui n'est évidemment pas suffisant !

Cependant, je pense que le régulateur n'est pas très regardant par rapport à tout ça car il s'est bien rendu compte, au fur et à mesure, que d'un point de vue technique, c'était pratiquement impossible de sortir toutes les informations requises en 72 heures.

C'est tout de même toujours utile de savoir que la possibilité existe, également pour Facebook. Chaque utilisateur est donc en droit de réclamer ses informations personnelles, et de les « récupérer », même si ce n'est jamais vraiment le cas... Les données qui ont transitées sur des sites dont l'utilisateur n'a même pas conscience sont irrécupérables, c'est trop tard, le mal est fait.

A : J'aimerais enchaîner avec des questions plutôt portées sur l'aspect marketing, si ça vous va. Ma question est la suivante : *selon vous, la publicité ciblée constitue-t-elle un outil de marketing numérique performant ?*

I : Avant le covid ou après le covid ? Parce que le virus a réellement eu un impact. Pour prendre un exemple sur Gmail, d'un point de vue utilisateur (je vais parler de ma propre expérience) : un matin je me suis connectée, et j'ai découvert que j'avais désormais ma boîte mail principale, une boîte « réseaux sociaux », une boîte « update », et enfin une boîte « forum ». J'ai vu ces 4 onglets apparaître et je me suis demandée de quoi il s'agissait, surtout que tous mes mails étaient déjà classés. Dans la boîte mail principale, je recevais, en toute logique, les mails de mes contacts. Dans la boîte réseaux sociaux, je recevais toutes les notifications de mes différents réseaux sociaux. Ensuite, je recevais les notifications pour tous les sites de commerce où j'avais laissé mon adresse e-mail. Les update concernaient quant à

eux les notifications, par exemple pour une facture à payer. En réalité, ils ont repris la boîte spam et l'ont mieux préfiltrées pour les utilisateurs.

D'un point de vue entreprise, avant ça n'avait pas d'importance, car il était évident que le mail allait se retrouver dans la boîte mail principale du client. Sauf qu'aujourd'hui, c'est terminé, il y a un tri qui est fait, même concernant la publicité ciblée par mail.

Il y a également la publicité ciblée par affichages, avec des « *banners* », des vidéos sponsorisées, etc. Selon moi, la publicité ciblée peut se montrer intéressante si et seulement si l'entreprise l'utilise de manière pertinente. En outre, il est indispensable que les algorithmes qui se cachent derrière soient très personnalisés, pour que le ciblage soit réussi.

A : Suite à la question précédente, j'aimerais rebondir en vous demandant : *quels sont, selon vous, les avantages et les inconvénients de la publicité ciblée ?*

I : D'un point de vue marketing, en ce qui concerne les avantages : on se rapproche du consommateur, on a des informations qui sont beaucoup plus performantes sur lui et un retour de sa part qui est également plus engageant.

En ce qui concerne les inconvénients et ce qui est compliqué pour l'entreprise, c'est de gérer la fréquence du contact avec le client. On ne peut pas toujours le bombarder, sinon le risque est qu'il en ait ras-le-bol. En d'autres termes, les fréquences des campagnes ne sont pas toujours faciles à organiser. La structure et la récolte des données pour le ciblage sont également un challenge. On revient à la couche intermédiaire de l'iceberg, si l'architecture interne n'est pas bien pensée, ça ne va pas fonctionner. C'est également un processus coûteux.

A : Une autre question que je me pose est celle-ci : *pensez-vous que les consommateurs soient particulièrement sensibles à la publicité ciblée ? Ou d'autres stratégies numériques sont-elles plus rentables ?*

I : D'après moi, les consommateurs préfèrent les recommandations de leurs réseaux, de leurs proches, de sites Internet spécialisés, ou même d'autres consommateurs. Par conséquent, d'une manière générale, je dirais que ce n'est pas prisé par les utilisateurs, notamment car ils

sont dérangés dans leur navigation. En bref, c'est le marketing de contenu et de communauté qui est préféré par les clients, surtout pour une relation de longue durée. C'est ce qui fait que les utilisateurs restent sur le long terme, même si c'est réellement un investissement.

A : On peut par conséquent dire que le choix est vite fait ?

I : Pas forcément, car le choix varie toujours en fonction de l'entreprise. On est dans une période un peu particulière, qui est déroutante. Je pense que post-covid, les publicités ciblées ne vont plus être possibles, car les gens vont encore plus se tourner vers du marketing de contenu et de communauté.

Dans le budget d'un ménage, on ne peut avoir de recul qu'après 3 mois et c'est donc maintenant qu'il faut entrer en contact avec les gens pour savoir comment ils ont consommé pendant le confinement. C'est certain que le comportement des consommateurs a complètement changé. Il y a un rapprochement au « *local* », qui est assez conséquent, on ne peut pas le nier. Qui dit rapprochement au local dit ancrage dans les valeurs humaines. On veut également pouvoir surfer en ligne et ce, de manière sécurisée et rapide. Il y a un énorme travail à faire pour les entreprises pour satisfaire leurs clients post-covid.

Par exemple, des grands magasins comme Zara ou Victoria Secret sont actuellement en train de déposer les bilans, et doivent fermer certains magasins, justement parce qu'ils n'ont pas su assurer le service en ligne.

Il y a également le fait que les individus n'ont plus envie d'acheter des choses jetables. C'est un sujet sociétal, et le confinement a laissé du temps pour que les gens prennent conscience de la situation. Finalement, le fait que les gens ne puissent plus aller acheter des choses a poussé à la créativité. Pour moi, on va revenir à quelque chose de beaucoup plus sain. Comme je l'ai dit, je pense que le marketing de contenu et de communauté va vraiment prendre le dessus sur la publicité ciblée.

A : La prochaine question que j'aimerais vous poser est celle-ci : *à l'époque, quelle a été la réaction des consommateurs face à la mise en place du RGPD ?*

I : Les consommateurs n'ont pas compris ce qu'il se passait : « *comment ça, maintenant je suis obligé d'accepter les cookies pour naviguer ?* ». C'est un peu tombé du ciel, cela a été assez compliqué par manque d'éducation.

Ensuite, on demande aux consommateurs de signer quelque chose, sans l'avoir vraiment lu. En fait, il y a un choix : soit l'internaute accepte, soit il relit, et grâce à sa relecture, il peut modifier des critères. Pour la majeure partie des gens, c'est incompréhensible ! C'est très compliqué et fastidieux de vulgariser toute la théorie.

Il faut savoir que le régulateur imposait aux entreprises d'ajouter un onglet qui permettait au consommateur de gérer sa relation client avec la marque. Imaginons que tu es sur ton compte personnel Zara et il est écrit « *pour la communication des informations promotionnelles, par quel canal voulez-vous être contacté ?* » et tu cochais par exemple SMS et e-mails. Tu encodes ton numéro de téléphone et ton e-mail. S'en suivait une autre question : « *pour tout ce qui est informations relatives aux contenus marketing, comme les conseils mode et déco, comment voulez-vous être contacté ?* ». En fait, pour chaque type d'interaction avec le client, l'entreprise était obligée de lui demander un e-mail, un numéro de téléphone, ou autre. C'était également quelque chose de fastidieux pour le client, et ce n'était pas facile de lui expliquer cela. Le défi est vraiment d'adapter la loi de manière « *user friendly* ».

A : D'accord, merci beaucoup pour toutes ces précieuses informations et précisions. Je suis très heureuse que nous ayons pu discuter si longuement, parce que j'en ai appris énormément et je n'ai aucun doute sur la plus-value apportée à mon mémoire. Je vous souhaite un bel été, merci encore !

I : C'était avec plaisir, surtout n'hésitez pas à revenir vers moi si vous avez d'autres questions, j'y répondrai sans problème. À bientôt !

