UCLouvain

Faculté de droit et de criminologie

# Les données personnelles, une richesse encore longtemps sans maitres ?

*Un droit de propriété sur nos données personnelles, analyse d'une "fausse bonne idée"*

Auteur : Jonathan MEY
Promoteur : Alexandre CRUQUENAIRE
Année académique 2018-2019
Master en droit, finalité 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*.

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

# *Remerciements*

*Je tiens à remercier tout d'abord le professeur Alexandre Cruquenaire pour sa disponibilité, son attention dans la supervision et l'encadrement de ce travail. Ses remarques pertinentes et ses conseils avisés lors du choix de mon sujet furent essentiels pour mettre en œuvre ce travail.*

*Je remercie également les corps professoraux des facultés de droit de l'Université de Namur et de Louvain-la-Neuve pour ces belles et riches années que j'ai pu vivre au sein de ces facultés.*

*Je voudrais aussi dire merci à mes courageux parents pour leurs précieuses relectures.*

*Et pour finir un grand merci à Madleen pour son soutien tout au long de ce mémoire et de ce mois de juillet.*

# *Les données personnelles, une richesse encore longtemps sans maîtres ?*

*"If you are not paying for it, you're not the customer; you're the product being sold."*
*- Andrew Lewis*

## Introduction

L'entrée en vigueur du nouveau Règlement sur la protection des données personnelles[1] a donné lieu à de nombreux débats d'idées dans les médias en 2018. Durant le visionnage d'un débat télévisé sur le thème des données personnelles[2], nous avons découvert le collectif *Génération Libre*[3] et une de leurs membres, Isabelle Landreau. Durant les échanges, elle évoqua plusieurs fois leur proposition phare qui consiste à instaurer un droit de propriété sur les données personnelles afin de permettre au citoyen de se réapproprier ce type de données. Ce droit sur nos *data* nous donnerait une position de force face aux géants du web lors de négociations concernant nos données et permettrait d'obtenir une compensation financière en échange de leur collecte et de leur traitement. La volonté de ce collectif est de pousser le citoyen lambda à devenir un bon gestionnaire de ses données et de profiter à son tour de l'essor de l'économie numérique.

Cette idée qui apparaît à première vue comme une belle promesse pour tout un chacun ne doit pour autant pas être prise à la légère, les conséquences d'un tel choix de modèle de "protection" étant considérables. En effet, ce n'est pas pour rien selon nous que les membres de la CNIL française qualifient cette ambition de "fausse bonne idée"[4].

---

1 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119, 4 mai 2016, pp. 1 à 88 ; Ce Règlement général sur la protection des données (que nous abrégerons en RGPD durant la suite de ce travail) est applicable depuis le 25 mai 2018.

2 RT FRANCE, "Interdit d'interdire : A qui profite la collecte de nos données personnelles?", Diffusé en direct le 22 oct. 2018 (accessible sur *Youtube* en juillet 2019 depuis ce lien : https://www.youtube.com/watch?v=BWINrcIaXFA).

3 Think-tank libéral fondé en 2013 et présidé par Gaspard Koening.

4 A., CHERIF, "Etre propriétaire de ses données personnelles, une dangereuse illusion", *latribune.fr*, 2018. (disponible en aout 2019 sur https://www.latribune.fr/technos-medias/internet/etre-proprietaire-de-ses-donnees-personnelles-une-dangereuse-illusion-773398.html).

Nous verrons dans les pages qui suivent qu'une analyse approfondie de la situation est nécessaire pour y voir plus clair dans l'économie actuelle de la *data*. Il est sans nul doute permis de penser que le cadre actuel de protection de nos données personnelles est insuffisant ou inefficient (sur ce point-là nous rejoignons la position de *Génération Libre*). Cependant les réponses à apporter peuvent être diverses et méritent chacune un développement. Ce travail aura pour objectif d'examiner les trois pistes qui nous semblent les plus intéressantes ;

- la création d'un droit de propriété sur nos *data*,
- celle d'une continuité du cadre actuel et
- pour finir l'option de la mise en commun.

## *Prérequis : Qu'est-ce qu'une donnée ?*

Les données qui peuplent notre quotidien sont très variées et peuvent être classées en différentes catégories. Elles forment, ensemble, ce qu'on appelle communément le "*big data*". Cette nouvelle approche, décrite plus en détail dans le point suivant, nécessite un volume gigantesque de données pour arriver à des résultats satisfaisants. Ce faisant, une quantité énorme de données[5] qui étaient ignorées ou supprimées par le passé car elles n'intéressaient personne sont actuellement stockées dans de gigantesques *data centers*. Cette masse de *data* y attend un futur traitement susceptible de rapporter un gros bénéfice financier à ceux qui les collectent.[6]

Le cadre légal européen qui régit les questions touchant aux données est assez complexe à l'heure actuelle[7]. C'est pourquoi nous allons rapidement définir ici les principales catégories de données afin d'y voir plus clair et distinguer plus facilement ce qu'est une donnée personnelle.

5 Il s'agissait de types de données divers, comme vos données de connexion, vos recherches et habitudes d'achat sur le web, les données de localisation émisses par votre smartphone, etc.

6 A., STROWEL,"Titre 10 - Les données des ressources en quête de propriété" in *Droit, normes et libertés dans le cybermonde*, Bruxelles, Éditions Larcier, 2018, pp. 251-268.

7 **L'Annexe n°1** (présente en fin de travail à la page 82 apporte un bon exemple de la diversité de cas imaginables dans la pratique et de l'importance d'une bonne qualification de la donnée par le juriste en amont.

La donnée personnelle est définie dans l'article 4, 1), du RGPD comme *"toute information se rapportant à une personne physique identifiée ou identifiable"* (...). *" Est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.*

Il y a au moins deux points très importants dans cette définition. Tout d'abord la donnée doit concerner une personne physique et ensuite elle doit pouvoir faire le lien entre cette personne et ladite information. Il est d'ailleurs intéressant de noter que le RGPD élargit la notion de donnée personnelle par rapport à son prédécesseur, la directive 95/46/CE, pour mieux protéger les individus contre le profilage et le ciblage publicitaire. La condition n'est plus qu'il soit possible de reconnaître l'identité de la personne mais bien que cette personne soit "individualisée", c'est-à-dire qu'elle puisse être identifiée grâce à d'autres données récoltées par rapport à la masse d'individus. Selon K. Rosier, une utilisation de cookies peut permettre une telle individualisation car ils permettront de retracer une personne et son adresse IP grâce aux autres recherches effectuées sur internet et aux données ainsi générées.[8]

La donnée non-personnelle est traitée de manière totalement différente par les autorités européennes. Pour ce type de données, la commission entendait créer une cinquième liberté sur le marché unique européen après celles des personnes, des capitaux, des biens et des services. C'est chose faite depuis l'adoption du Règlement européen du 9 novembre 2018 sur la libre circulation des données à caractère non personnel dans l'Union européenne[9]. Les données visées par ce règlement sont définies[10] à contrario de la définition des données personnelles citée précédemment, ce qui amène à se poser la question de la cohabitation entre ces deux réglementations. Le Parlement européen a prévu cette hypothèse en affirmant qu'aucune

8 K., ROSIER, "Titre 12 - La notion de « donnée à caractère personnel » a-t-elle encore un sens dans la protection des données de communications électroniques" in *Droit, normes et libertés dans le cybermonde*, Bruxelles, Éditions Larcier, 2018, pp. 699-714.

9 Règlement (UE) 2018/1807 du parlement européen et du conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, *J.O.U.E.*, L 303, 28 novembre 2018, pp. 59-68.

10 Les données non personnelles sont définies à l'article 3, 1) du Règlement sur les données non personnelles 2018/1807.

obligation de stocker les deux types de données séparément n'existait.[11] Si les deux types de *data* sont traitées en même temps, le Règlement de 2018 continuera à s'appliquer aux données non personnelles à moins qu'elles soient inextricablement liées ; dans ce cas, il faudra suivre les obligations imposées par le RGPD.[12] L'Union européenne confirme le principe de la libre circulation des données non personnelles par l'interdiction de tout principe de *''localisation des données''*[13] présent à l'article 3, 5) du Règlement de 2018.[14]

En pratique la différence n'est pas toujours aisée, c'est pourquoi les instances européennes se servent d'exemples pour préciser la notion de donnée non personnelle. Il peut ainsi s'agir des données relatives aux besoins de maintenance des machines industrielles ou de données améliorant l'agriculture de précision (optimisation de l'utilisation d'eau et de pesticides). Il semblerait également que la Commission cherche à l'heure actuelle un moyen de réduire le champ d'application très large des données personnelles pour accorder une place plus importante à son principe de "*free flow of data*". Le conseil à donner aux entreprises resterait de considérer, en cas de doute, une donnée comme personnelle pour éviter les sanctions prévues en cas de violation du RGPD.[15]

Les données "pseudonymisées"[16] et anonymes[17] sont légèrement différentes les unes des autres, les premières restent des données personnelles soumises au RGPD à moins de subir une anonymisation poussée qui empêcherait toute identification de la personne physique, tandis que

11 *Voy*. Considérant 10 du Règlement sur les données non personnelles 2018/1807.
12 *Voy*. l'article 2.2 du Règlement sur les données non personnelles 2018/1807.
13 Certains Etat-membres exigeaient la présence des données sur leur territoire (*localisation des données*). Cette pratique est désormais interdite pour ne pas faire obstacle à la libre concurrence.
14 O. HAYAT et L. HUIN, "Un régime juridique européen sur les données non personnelles", *Expertise*, janvier 2019, pp. 32-37 ; Règlement du 2018/1807 du parlement européen et du conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne ; C. FLYNN, "Shortcomings of the EU proposal for free flow of data", *InterMEDIA*, 2018, Vol 45, Issue 4, pp. 30-35.
15 O. HAYAT et L. HUIN, *op. cit.,* pp. 32-37 ; M. KNOCKAERT et T. TOMBAL, "Quels droits sur les données?", Conférence Actualités en droit du numérique, 42e session, Mons, mai 2019.
16 Une donnée pseudonymisée a subit un procédé de pseudonymisation, il s'agit selon l'article 4, 5) du RGPD, d'un traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires. Il faut pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.
17 D'après le considérant 26 du RGPD, une information anonyme est une donnée 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.

les secondes sont, par nature, exclues du champ d'application du RGPD. Attention, si une évolution technologique permet de retracer la personne physique derrière des données anonymisées, ces données redeviennent des données personnelles classiques et le RGPD doit par conséquent s'appliquer.[18]

Les secrets d'affaires sont protégés par la directive 2016/943/UE du 8 juin 2016[19] (simplifiée en "directive secrets d'affaires" dans notre travail) transposée en droit belge par la loi relative à la protection des secrets d'affaires publiée au Moniteur le 14 août 2018. Les "secrets d'affaires" protégés par la directive concernent les informations qui :

- "sont ***secrètes*** en ce sens que, (...) elles ne sont pas généralement connues des personnes appartenant aux milieux qui s'occupent normalement du genre d'informations en question, (...) pas aisément accessibles
- ont une ***valeur commerciale*** parce qu'elles sont secrètes,
- elles ont fait l'objet, de la part de la personne qui en a le contrôle de façon licite, de ***dispositions raisonnables***, compte tenu des circonstances, ***destinées à les garder secrètes***."[20]

Cette directive ne s'applique pas uniquement aux données, sachant que son champ d'application inclut également les données confidentielles répondant aux trois conditions susmentionnées. Le considérant 16 de la directive "Secrets d'affaires" précise que "les dispositions de la présente directive ne devraient créer aucun droit exclusif sur les savoir-faire ou informations protégés en tant que secrets d'affaires", il est donc acquis qu'aucun nouveau droit de la propriété intellectuelle n'a été introduit par la directive. Néanmoins celle-ci instaure une action en justice au titulaire de la donnée confidentielle (et donc un droit à agir à ce dernier) qui renforce grandement la protection effective de ce type d'informations. Cette reconnaissance d'un intérêt légitime à être protégé en justice constitue une avancée dans la défense des données confidentielles et instaure en pratique un quasi-droit de propriété sur ce type de données.[21]

18 *Voy*. le considérant 9 du Règlement sur les données non personnelles 2018/1807 et le considérant 26 du RGPD ; O. HAYAT et L. HUIN, *op. cit.*, pp. 32-37 ; M. MOURBY, E. MACKEY, M. ELLIOT, H. GOWANS, S. WALLACE, J. BELL, H. SMITH, S. AIDINLIS and J. KAYE, "Are «pseudonymised» data always personal data? Implications of the GDPR for administrative data research in the UK", *Computer Law & Security Review*, 2018, n°34, pp. 222-233.

19 Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, *J.O.U.E.*, L 157, 15 juin 2016, pp. 1-18.

20 *Voy*. l'article 1 de la directive 2016/943 (nous soulignons dans le texte)

21 A. STROWEL, *op. cit*., pp. 251-268.

Dans le cadre de ce mémoire, l'objectif sera de débattre de la question d'une patrimonialisation des données personnelles. Dans la suite de ce travail, nous allons donc recentrer le débat sur cette thématique après ce rapide tour d'horizon des possibles.

## *Pourquoi la data est-elle si importante ?*

Les nouvelles méthodes d'apprentissage de l'intelligence artificielle (*machine learning* ou *deep learning* notamment) et les entreprises de marketing sont les bénéficiaires les plus évidents de l'ère du big data. Ces technologies ne se basent plus sur de grandes théories ou des expériences uniques pour être efficaces mais plutôt sur l'analyse d'un nombre élevé de corrélations et de paramètres qui permettent de créer ou de prédire un résultat. Par exemple une IA peut apprendre, en analysant une base de données suffisamment fournie, à reconnaître des photos de chambres à coucher différemment agencées. La machine aura appris d'elle-même quelles sont les caractéristiques d'une chambre (la présence d'un lit, d'une commode, etc.) et arrivera, avec plus ou moins de succès, à reproduire d'elle-même une pièce inédite.[22] Les entreprises de marketing, elles, utilisent des données pour créer des profils types de consommateur ou pour prédire nos futures préférences de vote à partir de nos données personnelles. Elles sont de plus en plus utilisées par les équipes de campagnes électorales qui ne vont par exemple plus faire du porte à porte dans les quartiers considérées comme "trop peu rentables" (sous-entendu peuplées par une population trop peu amenée à voter pour son candidat) pour se focaliser plutôt sur les indécis. L'utilisation de la publicité ciblée sur Facebook lors de campagnes électorales a également explosé ces dernières années, grâce aux bons résultats qu'elle procure (pour illustration : réussite du *Brexit*, élection de Jair Bolsonaro au Brésil, etc.[23]) tout en amenant son lot de scandales durant certaines élections récentes. (Affaire *Cambridge Analytica* à la suite du *Brexit* par exemple).[24]

---

22 SCIENCEETONNANTE , "Le deep learning - Science étonnante #27", mis en ligne le 8 avril 2016 (disponible sur *Youtube* en aout 2019 depuis ce lien : https://www.youtube.com/watch?v=trWrEWfhTVg).

23 A. FALJAOUI, "Comment WhatsApp et Facebook ont influencé l'élection au Brésil", publié le 5 novembre 2018 sur *rtbf.be* (disponible depuis ce lien : https://www.rtbf.be/classic21/article/detail_comment-whatsapp-et-facebook-ont-influence-l-election-au-bresil?id=10064682) ; AFP, "Facebook étudie l'impact des réseaux sociaux sur les élections", publié le 30 avril 2019 sur *latribune.fr* (disponible depuis ce lien : https://www.latribune.fr/technos-medias/facebook-etudie-l-impact-des-reseaux-sociaux-sur-les-elections-815752.html).

24 P., MOURON, "Pour ou contre la patrimonialité des données personnelles", *Revue Européenne des Médias et du Numérique,* n°46-47, printemps-été 2018, pp 1-2.

Pour arriver à des résultats aussi impressionnant, l'important n'est pas réellement la pertinence de la donnée qu'on donnera aux algorithmes mais plutôt le volume qu'on réussit à collecter. Un programme va pouvoir identifier un certain nombre de corrélations dans ces données brutes pour découvrir un modèle (*pattern* en anglais) qui servira de base de travail à une hypothétique innovation. [25]

En 2013, des informations générales sur une personne comme l'âge, le genre ou la géolocalisation, coûtaient environ 0,50 $ pour mille personnes (soit 0,652 €). Les données d'une personne qui achète des voitures, des produits financiers ou qui part en vacances, valaient déjà un peu plus lorsqu'on les revendait à des entreprises qui produisent les biens qu'ils recherchent.[26] En 2015, le prix du fichier reprenant les données personnelles basiques de mille personnes n'avait pas réellement changé. Cependant le prix pour des profils plus détaillés et plus ciblés peut actuellement s'élever jusqu'à des sommes aux alentours de 250€ (prenons, par exemple, le cas d'une liste reprenant les données sensibles de personnes en surpoids qui intéresserait des entreprises pharmaceutiques vendant des produits amincissants). [27] Le commerce de la "donnée brute" ne rapporte donc en général pas de gros montants à l'unité.

La donnée brute n'est peut-être pas le nouvel or noir mais elle sert néanmoins de contrepartie à la majeure partie des services gratuits que nous utilisons sur internet. Nos données personnelles y sont récoltées, traitées et interconnectées avec d'autres informations pour ensuite permettre leur exploitation ou leur vente aux publicitaires. Ce sont les étapes qui suivent la récolte qui apportent la réelle valeur ajoutée aux données et permettent à ce *Business model* de fonctionner. C'est actuellement le modèle privilégié par les entreprises du net (la culture du gratuit y étant très forte), car il permet de toucher un très large public rapidement, ce qui est souvent synonyme de succès, du moins à court terme. Il arrive cependant que ces nouveaux

25 A. STROWEL, *op. cit*., pp. 251-268 ; H. ZECH, "Data as a Tradeable Commodity – Implications for Contract Law", Josef Drexl (ed.), Proceedings of the 18th EIPIN Congress: The New Data Economy between Data Ownership, Privacy and Safeguarding Competition, Edward Elgar Publishing, Forthcoming, 2017, p. 2 (Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063153).

26 RÉDACTION DE MÉDIAPART , "Combien valent vos données personnelles ?", publié le 15 juillet 2013 sur *médiapart.fr* (disponible depuis ce lien : https://www.mediapart.fr/journal/economie/150713/combien-valent-vos-donnees-personnelles) ; E. STEEL, E., LOCKE, C., CADMAN, E., et FREESE, B., "How much is your personal data worth ?", publié le 12 juin 2013 sur *financialtime.com* (disponible depuis ce lien : https://ig.ft.com/how-much-is-your-personal-data-worth/).

27 V.-L. BENABOU et J. ROCHEFELD, *A qui profite le clic ? Le partage de la valeur à l'ère numérique*, Paris, Odile Jacob, 2015, p. 106.

acteurs ne respectent pas la législation en vigueur. Un certain nombre de créateurs d'applications Android ont été accusés en juin 2019 de collecter les données de leurs utilisateurs sans qu'ils n'aient été informés de la chose. Cette collecte était réalisée y compris dans les cas où les individus avaient refusé de donner leur consentement au préalable.[28] Cette pratique est évidemment en totale opposition avec les principes fondamentaux du RGPD.

Aujourd'hui la *data* est incontournable. L'exploitation des données est un terrain qui est nécessaire à un grand nombre d'innovations à venir. Certains, comme des Sergei Brin, des Larry Page ou des Mark Zuckerberg, l'ont bien compris, alors que les européens sont généralement plus à la traîne.[29] Toutes ces données permettent donc à certains (Les *GAFAM* ou *BATX* en particulier[30]) d'exercer un pouvoir immense, de rester leaders dans beaucoup de domaines technologiques et d'amasser des profits colossaux (le chiffre d'affaires de Google s'élevait à plus de 110 milliards de dollars en 2017, sachant qu'il est en majeure partie constitué de revenus publicitaires[31]).

Ne serait-il pas plus équitable qu'une partie de ces montants revienne aux *data subject* originels des données ? Ou, comme le soutient le collectif *Génération Libre*, ne faudrait-il pas instaurer un réel droit de propriété sur ces données ? Dans le futur, allons-nous nous retrouver à payer avec nos données personnelles sur internet ?

28 J. REARDON, A. FEAL, P. WIJESEKERA, A. ELAZARI BAR ON, N. VALLINA-RODRIGUEZ and S. EGELMAN, "50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System", submitted to FTC PrivacyCon2019, 18 p. available at : https://www.ftc.gov/system/files/documents/public_events/1415032/privacycon2019_serge_egelman.pdf).

29 A., STREEL, "Titre 4 - Les données, l'innovation et le droit des concentrations" in *Droit, normes et libertés dans le cybermonde*, Bruxelles, Éditions Larcier, 2018, p. 109-116.

30 L'acronyme GAFAM fait référence aux géants du numérique américains : Google, Apple, Facebook, Amazon et Microsoft tandis que l'acronyme BATX fait référence aux géants du numérique chinois : Baidu, Alibaba, Tencent et Xiaomi.

31 T. HERPIN, "[Infographie] Les GAFAM et la répartition de leur chiffre d'affaire en 2017", 25 avril 2018 sur *ecommerce-nation.fr* (disponible depuis ce lien : https://www.ecommerce-nation.fr/gafam-repartition-chiffre-daffaires-2017/) et voir **l'annexe n°3** à la page 83 reprenant les bénéfices des GAFA M en 2017.

# Titre I : La thèse de la propriété privée

## *Chapitre 1 : Pour quelles raisons créer une propriété de la donnée, quels seront les avantages ?*

Section 1 : Profiter du marché actuel des données personnelles

L'intérêt le plus régulièrement mis en avant par les partisans d'un nouveau droit de propriété est d'ordre économique. Il s'agirait de permettre à chaque personne de prendre part au commerce très lucratif des données et de participer à un vrai marché réglementé.[32] Une relation privilégiée entre personnes "connectées" et entreprises existe en quelque sorte déjà et ces auteurs en sont bien conscients ! Quand on transmet nos données à notre assurance pour prouver qu'on est une personne saine et sportive afin obtenir une ristourne sur notre police d'assurance, on utilise nos données dans le but d'obtenir un avantage financier.[33] Il ne s'agit pas d'une vente mais l'usage qui est fait de nos données poursuit un but financier.

Un marché de la donnée à caractère personnel à proprement parler est déjà en place. Il est actuellement organisé en marché primaire, secondaire et tertiaire et c'est cette organisation que la majorité de la doctrine entend remettre en cause[34].

Le marché primaire concerne la collecte des données. Il s'agit d'échanger des données personnelles d'individus contre des services provenant de sociétés commerciales, d'administrations ou d'associations. Ces *data* ont certes une valeur économique mais sommes-nous vraiment en présence d'un marché ? En effet, les individus ne sont pas juridiquement vendeur de leurs données mais uniquement des sujets consentant au prélèvement et à l'utilisation de leurs données. Par contre, il y a bien une transaction contre une contrepartie, à savoir l'accès à un service "gratuit" contre l'accès aux données. Nous ne sommes donc pas en

32 A. BENSOUSSAN, "Pour un droit de propriété et une monétisation des données personnelles", *blog.lefigaro.fr*, février 2018.

33 G. MALGIERI and B. CUSTERS, "Pricing privacy: the right to know the value of your personal data", *Computer Law & Security Review*, 2018, n°34, pp.289-303.

34 C. DESCHANEL, "L'instauration d'un droit de propriété des données personnelles : vrai danger ou fausse utilité?", *R.L.D.I.*, février 2019, n°156, p. 37 ; A. RALLET, "Valoriser ses données personnelles ? 3 scénarios", *Document de travail*, Université de Paris Saclay, octobre 2018, 21 pp. 2-6 (disponible en août 2019 sur https://hal.archives-ouvertes.fr/hal-01909650/document) et *Voy.* schéma de **l'Annexe n°2** page 83.

présence d'une vente classique mais plutôt dans un système d'échange entre deux types de biens, chacune des parties ayant des besoins différents (utilisation d'un service en ligne pour l'un, collecte de données pour mettre en place ce service et le rentabiliser pour l'autre).

Le marché secondaire, lui, concerne les interactions entre les collecteurs de données (Facebook, une application mobile, etc.) et les agrégateurs de données (les *data brokers*). Il s'agit cette fois d'un vrai marché, les assemblages de *data* brutes sont échangés contre un certain prix entre un acheteur et un vendeur. A cette étape, le vendeur dispose généralement d'un droit de propriété sur l'ensemble des données, le droit *sui generis*[35]. Cela permet une meilleure maîtrise des données par les collecteurs et permet de les céder aux *data brokers* à leurs conditions (licences, droit d'accès ou droits d'utilisation). Ici, les *data* brutes sont transformées, elles sont organisées et traitées pour constituer des bases de données renfermant quantités d'informations statistiques sur une masse d'individus. Les courtiers ou *data brokers* sont la pierre centrale de ce second marché : ils ne sont pas forcés de se fournir en données auprès des collecteurs du marché primaire. Ils peuvent aussi plus simplement racheter les stocks de leurs collègues. En 2014 par exemple, la FTC (*Federal Trade Commission*) avance dans un rapport que sur 9 *data brokers*, 7 se fournissent principalement auprès d'autres intermédiaires plutôt qu'auprès des sources originelles, les collecteurs primaires.[36]

C'est dans la dernière phase, le marché tertiaire, que la *data* acquerra un maximum de valeur. Les *data brokers* vont travailler les données ("Tel un joaillier qui taille et unit ds pierres précieuses pour en faire un bijou") pour constituer *in fine* des profils de consommateurs ou d'individus. Les courtiers vont décupler la valeur des données en accomplissant ce travail d'assemblage et de profilage. Ce sont ces profils finaux qui intéressent les entreprises commerciales, qui sont en grande partie des annonceurs publicitaires agissant dans un souci d'optimisation de stratégies marketing. Plusieurs opérations sont possibles pour vendre les profils aux entreprises : la plupart du temps cela s'effectue sous forme de vente d'un service commercial (tel qu'une campagne marketing pour le compte d'une société x) tout en conservant la maîtrise des données, atout stratégique dans ce genre d'opération.[37] Tout ce processus est accompli pour améliorer les profits ou diminuer les coûts de l'entreprise ayant recours au *big*

35 Il ne s'agit pas d'un droit sur la donnée mais sur l'ensemble du contenu de la base de données. Il faut pouvoir démontrer une originalité dans le choix et la disposition des éléments constitutifs de la base de données.
36 C. DESCHANEL, *op. cit*., p. 37 ; A. RALLET, *op. cit*., pp. 2-6.
37 *Ibidem* ; *Ibidem*.

*data*. La valeur créée par la mise sur le marché des profils d'individus permet ensuite de déterminer rétroactivement les sommes qui devront être allouées aux étapes antérieures à la dernière métamorphose des *data*. On notera que les grands gagnant de ce système sont généralement les *data brokers*.

C'est en partant de ce constat que certains voudraient accorder aux personnes physiques originels le droit de devenir les "*traders*" ou "*data brokers*" de leurs données à caractère personnel.[38] Ces auteurs partent d'un postulat de base qui ressemble à un sentiment de résignation face à l'organisation actuelle du marché des données. Il leur semble irrémédiable qu'on puisse tracer et collecter la grande majorité de nos activités en ligne.[39] La seule solution à ce problème serait, selon ce point de vue, de mieux réglementer le système actuel. L'objectif principal d'une telle vision du marché des données semble être d'éviter les scandales liés aux activités des *data brokers* (comme le bien connu, et déjà cité, cas de l'Affaire *Cambridge Analytica* en 2018, qui devrait coûter plusieurs milliards à Facebook[40]) tout en combattant également l'injustice de l'actuelle répartition des richesses plutôt que repenser le système en profondeur.[41]

Certains constats des partisans de la patrimonialisation des données ne sont néanmoins pas dénoués de tout fondements, au contraire. Ainsi, les négociations au niveau du marché primaire sont pour l'instant clairement inéquitables. Les *data subjects* n'ont quasiment aucun pouvoir face aux géants de l'industrie et deviennent des "machines à consentement",[42] un des principaux problèmes étant l'asymétrie des positions lors de la transaction. En effet, les individus vont fournir des données brutes ayant peu de valeurs en elles-mêmes tandis que les *data brokers* de l'autre côté de la chaîne utiliseront ces données dans des modèles à bien plus forte valeur marchande. Un acteur du marché (le courtier) a une plus grande facilité à valoriser son produit que l'autre (les utilisateurs des services en ligne, "titulaires" de données).

38 A. BENSOUSSAN, *op. cit*.
39 *Ibidem*.
40 BELGA, "Facebook : le régulateur américain en faveur d'une amende de 5 milliards de dollars", 12 juillet 2019 sur lesoir.be (disponible depuis ce lien : https://www.lesoir.be/236331/article/2019-07-12/facebook-le-regulateur-americain-en-faveur-dune-amende-de-5-milliards-de-dollars?).
41 C. DESCHANEL, *op. cit*., p. 37.
42 N. PURTOVA, *Property right in personal data : a European perspective*, Alphen aan den Rijn, Kluwer, 2012, p. 54.

Au-delà de ces questions relatives au marché, il y a également, pour un certain nombre d'auteurs, un problème d'effectivité des normes européennes actuelles qui devraient être améliorées.[43]

Une des premières militantes de la propriété des *personal data*, Nadezhda Purtova, considère aussi qu'il est important de rééquilibrer le rapport de force entre les utilisateurs lambda d'internet et les *data controllers*. Pour elle, l'effet *erga omnes* de la propriété classique pourrait aider.[44] Il s'agirait de permettre ainsi de faciliter les actions en réparation de dommages lorsqu'une violation de la protection des *data* a lieu. Il suffirait d'attaquer n'importe qui (effet *erga omnes)* dans la liste des personnes impliquées dans le traitement des données pour obtenir réparation. Cela me semble peu réaliste actuellement mais cela serait très intéressant en pratique (par exemple dans les cas où il n'est pas évident de savoir à quel niveau du traitement la protection de la *data* fut violée ou par quel acteur de la chaîne de contrats).[45]

## Section 2 : Protéger la vie privée des utilisateurs

Une seconde série d'arguments en faveur de la propriété des données peut, assez ironiquement, étayer la thèse qu'il s'agit d'une avancée pour la protection de la vie privée. En poursuivant ce modèle, on pousserait les entreprises à utiliser moins de données car leur prix augmenterait certainement si les individus obtenaient une meilleure rémunération. Les acheteurs du marché tertiaire (sociétés de communication, marketing ou autres) n'auraient plus le budget pour acheter de la *data* à tout va. On pourrait ainsi facilement imaginer que cette diminution du nombre de données stockées par les grandes entreprises aurait pour conséquence d'améliorer la protection de la vie privée.[46] Cet argument est également valable, dans une moindre mesure, pour viser une meilleure protection de l'environnement. Les *data centers* sont en effet les gros pollueurs "invisibles" du net.[47] En réduisant la quantité de données en

43 *Ibidem*, p. 245.
44 *Ibidem*, pp. 250-251.
45 *Ibidem*, p. 252.
46 Y. PADOVA, "Entre patrimonialité et injonction au partage : la donnée écartelée? (Partie I)", *R.L.D.I.*, janvier 2019, n°155, pp. 47-56.
47 S. SERMONDADAZ, "Numérique et écologie : les data centers, des gouffres énergétiques ?", 9 mars 2018 sur *sciencesetavenir.fr* (disponible depuis ce lien : https://www.sciencesetavenir.fr/high-tech/informatique/numerique-et-ecologie-les-data-centers-des-gouffres-energetiques_121838) et J.-C. VERSET, "Internet bientôt premier consommateur mondial d'électricité", 10 avril 2018 sur *rtbf.be* (disponible depuis ce lien : https://www.rtbf.be/info/economie/detail_internet-bientot-premier-consommateur-mondial-d-electricite?id=9889099).

circulation et en poussant les professionnels à ne stocker que les données les plus pertinentes, on ferait collectivement un effort contre le réchauffement climatique.

Il existe en outre une grande différence de cultures juridiques par rapport à la question de l'interaction des *data* et de la protection de la vie privée. Aux États-Unis, on a plus facilement envie de défendre la vie privée grâce au droit de propriété tandis qu'en Europe, on a plutôt tendance à se baser sur les droits de l'homme ou les droits de la personnalité.[48]

Le *business model* de la collecte à grande échelle des données a prouvé son efficacité avec le temps. Pourrions-nous imaginer un nouveau système où les individus pourraient bénéficier du *big data* tout en maitrisant son fonctionnement et en contrôlant leurs propres données ?[49] De plus en plus de voix s'élèvent pour tendre vers cet idéal, surtout aux USA et au Royaume-Uni, en prônant diverses solutions. Si l'on décide de suivre les recommandations des adeptes de la patrimonialisation, le pouvoir central sur la collecte et l'utilisation des *data* reviendrait aux individus. Permettre de sélectionner quelles données seront partagées et celles qui resteront privées rentrerait par exemple dans la même optique. Tout comme contrôler les différents usages ultérieurs de nos informations personnelles dans les différentes étapes du traitement. On se rend compte qu'une grande partie de ces souhaits sont déjà mis partiellement ou totalement en œuvre dans l'Union Européenne (par l'intermédiaire de principes tels que le droit à l'oubli, le droit à la portabilité, le droit de rectification, etc.), ce qui fait du droit communautaire le droit le plus proche des désirs exprimés par les défenseurs d'un droit de propriété sur nos données.[50]

En suivant cet argumentaire on arrive à la conclusion que si le marché fonctionnait plus efficacement (sous-entendu, si chacun contrôlait ses données avec un droit de propriété et pouvait les échanger), il y aurait moins d'invasions de la vie privée des individus.[51]

---

48 J.E.J. PRINS, "The propertization of personal data and identities", *Electronic Journal of Comparative Law*, vol. 8.3, october 2004, p. 2 (available at https://www.researchgate.net/publication/247957565_The_Propertization_of_Personal_Data_and_Identities) ; Y. POULLET, "Le fondement du droit à la protection des données nominatives : «Propriétés ou Libertés»", Nouvelles technologies et propriétés, novembre 1989, pp. 175-205.

49 I. RUBINSTEIN, "Big Data: The End of Privacy or a New Beginning?", *New York University School of Law Public Law & Legal Theory research paper series*, working paper n°12-56, october 2012, p. 1 (available at : https://ssrn.com/abstract=2157659).

50 I. RUBINSTEIN, *op. cit*., pp. 9-10.

51 J.E.J. PRINS, *op. cit*., p. 1.

Section 3 : Favoriser *l'empowerment* des individus

En pratique, les personnes physiques sont majoritairement la "partie faible" au contrat de service qu'ils concluent. Ils ne possèdent souvent pas assez d'informations ou de contrôle sur leurs données personnelles.[52] Permettre à la propriété des données de se développer permettrait d'augmenter la visibilité et notre connaissance de la collecte et du traitement des *personal data*.[53]

Et par-dessus tout, un auteur[54] affirme que le fait de refuser aux individus un droit de propriété sur leurs données les rendrait moins capable de négocier dans leur propre intérêt. Grâce à une propriété pleine et entière, les individus seraient libres de négocier les contenus des contrats avec les tiers de la manière qui leur convient et leur correspond le mieux. Il souhaite également qu'on pousse les individus à améliorer la gestion de leurs données et accroître leur responsabilisation sur le sujet (*active empowerment*).[55] Le Conseil d'État français regrettait en 2014 qu'à l'heure actuelle *"les droits reconnus aux individus se limitent, pour l'essentiel, à leur permettre de rester à l'écart du traitement de leurs données (choix qui n'est presque jamais fait) sans leur donner de réel pouvoir sur le contenu du service et la manière dont les données sont traitées."* La juridiction française nous montre par cet avis qu'elle considère aussi qu'une forme d'*empowerment* des individus plus aboutie est possible. Le RGPD n'a pas modifié en profondeur cette absence de choix à la disposition du consommateur, la critique reste donc d'actualité.[56]

Certains ne sont pas aussi "radicaux" dans leurs revendications, ils voudraient uniquement que l'on puisse connaître facilement la valeur de nos données avant de les céder. Être au courant de la valeur des informations qu'on s'apprête à donner pour accéder à un service permettrait de mieux peser le pour et le contre au moment de donner son consentement. Il est généralement plus simple pour des citoyens peu informés sur le sujet de comprendre et d'évaluer la situation quand on parle d'argent plutôt que masses de *data*.[57]

52 *Ibidem*, p. 4.
53 *Ibidem*, pp. 6-7.
54 *Ibidem*.
55 G. MALGIERI and B. CUSTERS, *op. cit*., pp.289-303.
56 C. DESCHANEL, *op. cit*., p. 39.
57 G. MALGIERI and B. CUSTERS, *op. cit*., pp.289-303.

Il s'agit là de nouveau d'un argument fort répandu auprès des partisans de la patrimonialisation des données et appuyé dans leurs discours. Le RGPD et son entrée en vigueur en 2018 ont eu pour effet de lancer (durant un temps du moins) un vrai débat de société autour de la gestion de nos *data*. Il est vrai que l'information des personnes est un pan crucial dans la mise en œuvre de la protection des données et on ne peut pas nier qu'il s'agit sans doute d'une des principales réussites de ce Règlement.

## Section 4 : le RGPD et le droit européen donnent un nouveau souffle à l'idée de propriété

Nous profitons déjà actuellement de nombreux services "gratuits" en ligne, mais pourrons-nous bientôt affirmer clairement qu'il s'agit de la contrepartie à l'acceptation du traitement de nos données ? Une proposition de Directive datant du 9 décembre 2015 a jeté un flou. Elle a pour objet d'établir des règles uniformes applicables aux contenus numériques et vise les cas où un consommateur obtient un service contre paiement mais également ceux où il s'agit d'une "contrepartie non pécuniaire", en précisant par exemple "sous la forme de données personnelles ou de toutes autres données".[58] Il s'agit de la première ouverture du droit européen à la possibilité d'utiliser ses données personnelles comme contrepartie contractuelle. Il faut néanmoins nuancer ce propos car l'actuel projet est encore susceptible de changer et la compatibilité d'un tel système avec le nouveau règlement de protection des données (RGPD) semble extrêmement compliquée en pratique.

Ce nouveau Règlement européen sert justement de nouvelle base d'arguments pour redonner vie au projet de propriété des données personnelles. Deux articles en particulier sont cités par *Génération Libre* comme étant des précurseurs d'un futur droit de propriété privée sur nos *data*, l'article 17 (*droit à l'oubli*) et l'article 20 du RGPD (*droit à la portabilité des données*).[59]

58 R. ROBERT, "Peut-on payer avec ses données personnelles : La proposition de directive « contenu numérique » introduit le ver dans le fruit", *J.T.D.E.*, 2017, n° 9, p. 356.

59 A. BENSOUSSAN, *op. cit.* ; I. LANDREAU, G. PELIKS, N. BINCTIN, et V. PEZ-PÉRARD, sous la direction de LÉGER, L., "Créer une patrimonialité des données à droit constant.", dans le rapport "Mes datas sont à moi." du collectif Génération Libre, janvier 2018, pp. 77-78 et 81. (disponible sur : https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf).

Le premier permet aux individus d'exiger, dans certaines conditions, l'effacement des données les concernant. Ce nouveau droit à l'oubli accordé aux citoyens trouve son origine dans un arrêt important de la Cour de justice européenne en 2014, *l'arrêt Google Spain*[60]. Le responsable de traitement doit mettre en œuvre des mesures raisonnables pour supprimer des informations nous concernant dans plusieurs cas, lorsque ;

- les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées,
- la personne concernée retire le consentement sur lequel est fondé le traitement,
- la personne concernée s'oppose au traitement et il n'existe pas de motif légitime impérieux pour le traitement,
- les données à caractère personnel ont fait l'objet d'un traitement illicite,
- les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre.

L'article 20 concerne lui le droit à la portabilité des données, qui permet aux individus de recueillir les données à caractère personnel qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine. Cet article accorde également le droit de transmettre ces données à un autre responsable de traitement sans que le premier responsable du traitement puisse y faire obstacle.

Ces deux articles consacreraient deux éléments essentiels de la propriété matérielle, l'*usus* et l'*abusus*. Le *fructus* étant alors le seul composant de la propriété manquant, c'est précisément celui-ci que les lobbys tels que Génération Libre entendent introduire en prônant l'exploitation et la collecte des "fruits" des données par les individus eux-mêmes.[61]

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

61 I. LANDREAU, G. PELIKS, N. BINCTIN, et V. PEZ-PÉRARD, sous la direction de LÉGER, L., *op. cit*., pp. 77-78 et 81.

Il est intéressant de noter que le groupe de travail Article 29 (devenu entretemps le "Comité européen de la protection des données") recommande lui aussi d'utiliser le RGPD pour rééquilibrer la balance économique entre les grands groupes industriels et les consommateurs, personnes physiques sujettes au traitement de données et d'ainsi partager la richesse créée par le *Big data*.[62] Pourquoi ne pas aller encore un peu plus loin dans la même idée dans ce cas ?

## *Chapitre 2 : Quels sont les idées concrètes/arguments proposés par Génération Libre et les autres auteurs favorables à la patrimonialisation des données personnelles ?*

La propriété privée des données est en réalité une vieille idée très vraisemblablement née aux USA au début des années 70'.[63] Il est possible de retrouver des documents où Y. Poullet combattait déjà cette idée au début de sa carrière dans les années 90'[64].

Les militants de *Génération libre* souhaitent qu'on puisse à terme appliquer le droit commun des biens aux données personnelles. Ils souhaitent rééquilibrer la chaîne de revenus issus des *personal data* commercialisées. Pour l'instant les *databrokers* américains (Acxiom et Bluekai en tête) écrasent le marché et favorisent les *GAFAM* dans la collecte de données. De grands partenariats sont par exemple conclus entre Facebook et 4 grandes sociétés de courtiers de données. Tout ce système est fort opaque et le concept de propriété pourrait justement y apporter de la transparence.[65]

L'objectif central, déjà annoncé dans ce travail, est de créer un gain qu'on pourrait retirer de la simple utilisation de nos données.[66] Vendre celles-ci selon nos préférences tout en gardant certaines informations privées permet de donner le choix aux individus dans la plus pure

62 P. DE HERT, V. PAPAKONSTANTINOU, M. MALGIERI, L. BESLAY, and I. SANCHEZ, "The right to data portability in the GDPR: Towards user-centric interoperability of digital services", *Computer Law & Security Review*, 2018, p. 195.

63 N. PURTOVA, "Property right in personal data: Learning from the American discourse", *Computer Law & Security Review*, 2009, n°25, p. 1.

64 Par exemple : Y. POULLET, "Les concepts fondamentaux de la protection des données et les nouvelles technologies de l'information", Dr. Infrom., 1987/4, pp. 222-227.

65 I. LANDREAU, G. PELIKS, N. BINCTIN, et V. PEZ-PÉRARD, sous la direction de LÉGER, L., *op. cit*., pp. 84 et 98.

66 Y. PADOVA, "Entre patrimonialité et injonction au partage : la donnée écartelée? (Partie I)", *R.L.D.I.*, janvier 2019, n°155, pp. 47-56.

tradition libérale. Pour l'instant, nous acceptons déjà de nous dévoiler gratuitement (remplir des formulaires d'inscriptions avec toutes nos coordonnées par exemple) : cette quête d'acquisition de nouveaux droits a donc réellement un sens.[67]

De petites *start-up* se lancent d'ores et déjà dans l'expérience de la commercialisation des données à petite échelle. Les premiers résultats sont néanmoins mitigés (voir point consacré à la question au chapitre 3).[68]

Actuellement il est difficile de savoir si les données sont considérées comme des contreparties dans les contrats qui nous lient aux principaux géants du net, que ce soit pour le simple consommateur ou pour les juges et régulateurs étatiques, les conditions d'utilisation et règles de confidentialité étant souvent confuses. Il faudrait clarifier tout cela une bonne fois pour toute.[69]

Il est également avancé que le marché prend déjà en compte le respect de la vie privée des individus. En effet, celui-ci répond à des demandes et les prend en compte si elles sont suffisamment importantes aux yeux des consommateurs (prenons par exemple *WhatsApp* qui a longtemps considéré la protection des communications via son application comme une de ses priorités avant son rachat par Facebook). Toujours selon le même auteur, si dans certains cas, la vie privée n'est pas assez protégée, cela signifie que les gens préfèrent prendre en compte l'efficacité et la prise en main plus simple de ce type de services de consommations.[70]

Une idée intéressante a été émise par G. Malgieri et B. Custers[71], qui souhaitent préciser la notion de "donnée personnelle". Pour eux, la *data* qui n'est pas intrinsèquement personnelle pourrait faire l'objet d'un droit de propriété, sans qu'on se retrouve dans une situation éthiquement problématique. Ces auteurs citent à titre d'exemple une idée émanant d'un arrêt de la *Federal Court of Australia,* selon lequel les adresse IP ne seraient pas des données sujettes (par défaut) à la protection de la vie privée.

67 A. BENSOUSSAN, *op. cit*.
68 Voir par exemple la star-up française "*My Data is Rich*" accessible à partir de ce lien https://mydataisrich.com/ (dernière connexion de notre part en juillet 2019)
69 R. ROBERT, *op. cit*., p. 357.
70 N. PURTOVA, "Property right in personal data: Learning from the American discourse", *Computer Law & Security Review*, 2009, n°25, p. 518.
71 G. MALGIERI and B. CUSTERS, *op. cit*., pp.289-303.

N. Purtova, auteure très prolifique sur le sujet, considère que les données sont des biens rivaux. D'après elle, la réelle question qu'on devrait se poser n'est pas "propriété des données à caractère personel" versus "pas de propriété" mais quel type de propriété on souhaite. En effet si on décide de ne rien faire, il est évidement que l'inaction profite aux grands du net qui assoient petit à petit leur emprise sur les données qu'ils saisissent depuis des années.[72]

Et enfin nous terminons l'examen des thèses de *Génération Libre* et ses alliés grâce à une thématique fort proche de notre sujet. Outre les éléments déjà cités, ils souhaitent mettre en place une TVA harmonisée au niveau européen sur les activités numériques qui "créent de la valeur grâce aux utilisateurs". Cette idée vient d'être mise sur pied par la France malgré que le projet soit bloqué au niveau européen, certains pays scandinaves étant actuellement défavorables au projet. La France a donc fait cavalier seul et court maintenant le risque de subir des sanctions de la part des États-Unis.[73]

## *Chapitre 3 : Quels sont les inconvénients de ce type de démarche et les critiques ?*

### Section 1 : La donnée personnelle unique n'a quasiment aucune valeur

Il est actuellement possible de trouver des données en abondance, sachant que la donnée à caractère personnel n'a de valeur qu'en grand nombre. Cette valeur augmente encore plus si cette information a pu subir un traitement et débouche sur un profilage qui la rend plus pertinente pour un type d'entreprise donné. Le profilage (stade ultime de l'utilisation d'une *data*)

72 N. PURTOVA, "The illusion of personal data as no one's property", *Law Innovation and Technology*, 2015, p. 84. (available at : https://www.tandfonline.com/doi/abs/10.1080/17579961.2015.1052646).

73 I. LANDREAU, G. PELIKS, N. BINCTIN, et V. PEZ-PÉRARD, sous la direction de LÉGER, L., *op. cit.*, pp. 96-98 ; Y. PADOVA, "Entre patrimonialité et injonction au partage : la donnée écartelée? (Partie II)", *R.L.D.I.*, février 2019, n°156, pp. 3-4 ; J. MASSARD, "Trump riposte à la « taxe GAFA » française", 11 juillet 2019 sur *euronews.com* (disponible depuis ce lien : https://fr.euronews.com/2019/07/11/trump-riposte-a-la-taxe-gafa-francaise) ; P. DUGUA, "Donald Trump attaque la France sur la taxe Gafa", 11 juillet 2019 sur *lefigaro.fr* (disponible depuis ce lien : http://www.lefigaro.fr/conjoncture/donald-trump-ordonne-une-enquete-sur-la-taxe-gafa-prelude-a-des-sanctions-20190711) et E. CONESA, "La France adopte la taxe GAFA malgré les menaces de Trump", 11 juillet 2019 sur *lesechos.fr* (disponible depuis ce lien : https://www.lesechos.fr/monde/etats-unis/la-france-adopte-la-taxe-gafa-malgre-les-menaces-de-trump-1037413).

a ainsi pour but premier de créer de la publicité ciblée pour chaque utilisateur d'internet et constitue une des bases principales du modèle économique utilisé par la majorité des *start-up* ou géants californiens du web.

Un certain nombre d'expérimentations sont déjà menées en pratique pour tester la viabilité d'un système reposant sur l'achat des données personnelles et il s'avère qu'on n'en retire que très rarement plus de quelques dollars par mois. Les projets qui sont déjà menés aujourd'hui ne sont donc pas très concluants...[74]

Les données valent de moins en moins d'argents avec le temps. En 2006 on pouvait vendre une donnée à 0,50 $, alors que maintenant sa valeur est descendue aux alentours de 0,05 $. Cette chute est en grande partie due au fait que les données personnelles sont bien plus nombreuses à être collectées aujourd'hui. Aux USA, où les données circulent bien plus librement qu'en Europe, les prix baissent aussi énormément.[75] Pris isolément, une donnée n'est finalement ni très utile, ni très rare.[76]

Aujourd'hui les *data brokers* disposent déjà d'une quantité énorme de données sur nous. D'après le texte *"Pricing privacy : the right to know the value of your personal data"* de G. Malgieri et B. Custers,[77] Acxiom leader US en la matière possèderait en moyenne 1500 données en rapport avec vous ou n'importe quel autre individu présent sur le net.

Une étude datant de 2012 réalisé par le *Boston Consulting Group* concluait que la valeur créée par l'exploitation des données serait de 1 000 milliards d'euros par an d'ici 2020 en Europe. Lorsqu'on se trouve face à ces chiffres, on comprend mieux la réputation de "nouvel or noir de la donnée". Viviane Reding, qui fut vice-présidente de la commission UE, affirme de son côté que l'économie des données représentait 315 milliards d'euros en 2011 et qu'elle pourrait exploser jusqu'à atteindre 1 trillion en 2020 ![78]

74 S. HARRISON, "Can you make money selling your data", 21 septembre 2018 sur *bbc.com* (disponible depuis ce lien : http://www.bbc.com/capital/story/20180921-can-you-make-money-selling-your-data) ; Y. PADOVA, "Entre patrimonialité et injonction au partage : la donnée écartelée? (Partie I)", *op. cit.*, pp. 47-56.

75 G. MALGIERI and B. CUSTERS, *op. cit*., pp.289-303.

76 M. MICHOT-CASBAS et C. HERVÉ, "Introduction - Les données massives en santé : enjeux éthiques des Big Dta dans la réalité des soins", dans *Innovation en santé publique des données personnelles aux données massives (big data),* Paris, Librairie générale de droit et de jurisprudence, 2018, p. 8.

77 G. MALGIERI and B. CUSTERS, *op. cit*., pp.289-303.

78 V.-L. BENABOU et J. ROCHEFELD, *A qui profite le clic ? Le partage de la valeur à l'ère numérique*, Paris, Odile Jacob, 2015, p. 29

Cependant, certains auteurs avancent qu'il est possible d'obtenir 11$ contre l'octroi d'une date de naissance, 25$ pour un profil complet aux USA et 40$ en Europe pour le même profil. Il s'agit là d'un montant non négligeable, d'autant plus intéressant lorsqu'on réalise qu'on donne déjà tous ces renseignements gratuitement actuellement.[79]

Section 2 : La donnée personnelle ne respecte pas les éléments essentiels du droit de propriété

On ne retrouve pas exactement les 3 attributs classiques et civilistes de la propriété ; *abusus, fructus* et *usus*.[80] De plus, la donnée est généralement un bien éphémère, qui peut changer rapidement.

L'*usus* est une autre appellation du droit de jouissance directe d'un bien accordé à celui qui le détient. Il est possible de l'appliquer aux données à caractère personnel, même s'il est difficile d'imaginer un *usus* sur les données d'autrui en cas de transfert de propriété. En effet, le tiers bénéficierait alors du droit d'utiliser ces données comme il le souhaite, ce qui n'est pas acceptable dans notre conception des données comme émanant de la personne d'un individu. Une telle utilisation d'éléments de la personne d'autrui pourrait alors constituer une forme "d'usurpation d'identité". [81]

Le *fructus*, quant à lui, est le droit de percevoir les fruits provenant du bien. Il n'y a pas de raison de ne pas appliquer cet élément de la propriété aux données personnelles. Toutefois, la section précédente démontre bien qu'actuellement les projets menés ne permettent pas de trouver dans les données une grande source de revenus sur la durée.[82]

Et enfin l'*abusus* constitue le droit de disposer de la chose comme on le souhaite, en choisissant de la détruire ou de la vendre par exemple. Appliqué aux données, cela permettrait au propriétaire d'un bien d'interdire à un individu d'accéder aux données, de les céder à un tiers

79 C. GATES et P. MATTHEWS, "Data is the New Currency", *NSPW '14 proceeding of the 2014 New Security Pardigms Workshop*, Victoria British Columbia Canada, 2014, p. 110.

80 P. MOURON, *op. cit*., p. 6 ; Y. PADOVA, "Entre patrimonialité et injonction au partage : la donnée écartelée? (Partie I)", *op. cit*., p. 50 ; F. MATTATIA et M. YAÏCHE, "Etre propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété? (Partie I)", *R.L.D.I.*, mai 2015, n°115, pp. 63-65.

81 P. MOURON, *op. cit*., p. 6 ; Y. PADOVA, "Entre patrimonialité et injonction au partage : la donnée écartelée? (Partie I)", *op. cit*., p. 50.

82 *Ibidem* ; *Ibidem*.

ou de les détruire. Il s'agit sans doute là de l'élément le plus problématique en lien avec une éventuelle propriété des données car il semble compliqué de transférer à un tiers le droit d'utiliser nos données et lui permettre de supprimer ainsi une part de notre "identité numérique". De plus, le caractère intangible et transmissible de la donnée est un frein considérable à la consécration d'un *abusus* et d'un *usus* sur celles-ci. Comme la donnée est facilement copiable et stockable, il n'est pas simple de s'assurer d'être plein propriétaire du bien et d'être le seul titulaire de l'*usus* et de l'*abusus*. Comment s'assurer que le précédent propriétaire n'en profite pas pour revendre une seconde fois la base de données à un concurrent ? Généralement il ne sera pas possible de s'en assurer. [83]

Entre des points de vue inconciliables il semble néanmoins exister une voie intermédiaire : On pourrait imaginer désacraliser l'absolutisme du droit de propriété et le faire évoluer pour qu'il s'adapte aux nouvelles caractéristiques de l'information numérique. La propriété de l'information n'est cependant pas souvent reconnue en pratique, que ce soit dans le monde civiliste ou anglo-saxon (comme rares exemples, nous pouvons citer une décision rendue par le tribunal de grande instance de Créteil le 23 avril 2013 et Oxford v. Moss).[84]

Le jugement du tribunal de grande instance de Créteil précédemment cité devait trancher une question épineuse : peut-on voler une donnée à caractère personnel ? Est-il possible d'en demander la récupération comme n'importe quel bien matériel et peut-on vraiment qualifier cela d'une soustraction matérielle d'une chose (alors qu'il s'agissait *in casus* de recopiages de données sans vol du support physique) ? Il n'existe pas de position unanime de la doctrine actuellement sur ce point[85], bien que cette question soit réglée en pratique depuis l'adoption de la loi du 28 novembre 2000 sur la criminalité informatique. Cette ancienne controverse met aujourd'hui en lumière les conceptions respectives du statut juridique à accorder aux données.[86]

---

83 P. MOURON, *op. cit*., p. 6 ; Y. PADOVA, "Entre patrimonialité et injonction au partage : la donnée écartelée? (Partie I)", *op. cit*., p. 50.

84 V.-L. BENABOU et J. ROCHEFELD, *op. cit*., pp. 52-56 ; Tribunal de Grande instance de Créteil, 11ème chambre correctionnelle, jugement du 23 avril 2013 ; *Ofxord v. Moss*, Divisional Court, Queens Bench (1979) 68 CR App Rep 183.

85 C. DESCHANEL, *op. cit*., p. 40 ; S. GUTWIRTH, et G. GONZALEZ FUSTER, "Titre 5 - L'éternel retour de la propriété des données de l'insistance d'un mot d'ordre" in *Droit, normes et libertés dans le cybermonde*, Bruxelles, Éditions Larcier, 2018, pp. 117-140 ; I. LANDREAU, G. PELIKS, N. BINCTIN, et V. PEZ-PÉRARD, sous la direction de LÉGER, L., *op. cit*., pp. 60-63.

86 C. DESCHANEL, *op. cit*., p. 40 ; S. GUTWIRTH, et G. GONZALEZ FUSTER, *op. cit*., pp. 117-140.

Nous ne développerons pas la controverse en détail mais nous bornerons à dire qu'il y a eu initialement un bon nombre de décisions belges[87] reconnaissant le vol de donnée ou de logiciels tout en constatant qu'il n'y avait pas de dépossession, le recopiage de ceux-ci étant donc suffisant pour constituer un vol. Il s'agit d'anciennes décisions généralement évoquées par les défenseurs d'un droit de propriété sur les données qui y voient une consécration de leur conception matérialiste, la donnée était alors traitée comme tout autre bien devant être protégé du vol.

Cependant la Cour de cassation finit par mettre de l'ordre dans sa jurisprudence[88] et considéra qu'il fallait rejeter cette interprétation de l'infraction de vol et se basera sur le principe important de l'interprétation stricte de la loi pénale (*nullum crimen, nullum poena sine lege*). Les faits n'étant pas compris dans la définition légale de l'infraction (pas de soustraction matérielle in casus), il n'est pas possible de les qualifier de vol.

Nous voudrions conclure en pointant le fait qu'il existe chez certains une forme de sacralisation de la propriété privée. La "libération de l'individu" que nous sommes supposés atteindre grâce à la propriété est sans nul doute exagérée, la propriété privée est également soumise à des limites en pratique (citons par exemple l'abus de droit ou plus simplement la difficulté qu'ont les droits intellectuels à combattre efficacement le piratage et la diffusion d'œuvres sur internet).[89]

## Section 3 : L'effet principal sera de renforcer la position des géants d'internet

La réelle conséquence de la mise en place d'un droit de propriété serait de sécuriser le fondement juridique de l'exploitation des données personnelles. Les collecteurs de données à caractère personnel pourront être certains d'en avoir le contrôle et de bénéficier de leur valeur financière en cas de cession ou transfert de propriété. Les vrais grands bénéficiaires de la mise en place d'un tel système ne seront donc pas les personnes physiques mais bien les entreprises ![90]

87 Par exemple : Anvers, 13 décembre 1984, *R.W.*, 1985-1896, pp. 244-246.
88 Cass., 11 septembre 1990, *Pas*, 1991, I, p. 37.
89 M. LAROCHE, "Vers un renouvellement de la propriété? Les fonctions du droit de propriété.", *Propriété(s) et données*, décembre 2016, Paris, France, pp. 1-2 (disponible en aout 2019 sur : https://hal.archives-ouvertes.fr/hal-02090602/).
90 Y., PADOVA, "Entre patrimonialité et injonction au partage : la donnée écartelée? (Partie I)", *op. cit.*, pp. 47-56.

Les individus risquent de perdre beaucoup en protection. Attiré par l'appât du gain, certains risquent de prendre de très mauvaises décisions sans pouvoir les modifier en raison du contrat de cession de leurs données.[91]

L'ancienne présidente de la Cnil, Isabelle Falque-Perrotin, qualifie la propriété des données à caractère personnel de "fausse bonne idée" dans le rapport d'activité de la Cnil de 2013 car *"à priori séduisante, cette démarche impose en réalité une grande prudence car la privatisation de ses données, et donc leur possible cession ou vente, revêt un caractère d'irréversibilité préoccupant pour l'individu. Les droits, une fois vendus, comment reprendre la main sur ses données ? A l'inverse, le droit actuel de la protection des données personnelles ouvre des droits à l'individu même lorsque ses données sont produites et traitées par d'autres"*.[92] Le Conseil d'Etat français a aussi rejeté la piste d'un droit de propriété des données personnelles dans son rapport de 2014 : il énonce ainsi que le droit de propriété deviendrait ainsi un droit d'être dépossédé et c'est donc le régime "personnaliste" actuellement en vigueur qui conserve sa préférence.[93]

Il est difficile d'imaginer qu'on puisse accepter de donner notre consentement pour une telle transaction selon les règles du RGPD en échange d'un service commercial. Les conditions sont tellement strictes qu'il semble impossible d'inclure celui du consommateur in casus dans les cas considérés comme valables. D'ailleurs le C.E.P.D. a rendu un avis sur la question où il rappelle clairement que *"les données à caractère personnel ne peuvent être considérées comme une contrepartie pour une demande de service, comme l'accès à un site web ou à une application"*.[94]

91 G. MALGIERI and B. CUSTERS, *op. cit*., p. 301.
92 F. MATTATIA et M. YAÏCHE, "Etre propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété? (Partie II)", *R.L.D.I.*, juin 2015, n°116, p. 44.
93 *Ibidem*.
94 R. ROBERT, *op. cit*., p. 357 ; Avis 7/2017 du C.E.D.P. sur la proposition de règlement relatif à la vie privée et aux communications électroniques, pp. 30-31.
.

Comment pourrions-nous appliquer une propriété des données en même temps que certains droits existants ? Il y aurait dans ce cas une disparition de certaines protections du RGPD : faut-il vraiment considérer cela comme un progrès ? Qu'adviendra-t-il, par exemple, de la possibilité actuelle de modifier une information (droit de rectification) ou du droit à mettre à jour nos données ? Cela serait-il toujours possible après les avoir aliénés et avoir perdu tout droit de regard ou faut-il justement en conclure que nous serions obligés de tenir nos données à jour ? Comment articuler ce nouveau système avec le droit à l'oubli également ? Toutes ces questions restent sans réponses dans les travaux des auteurs favorables au droit de propriété.

L'asymétrie d'information entre l'acheteur et le vendeur serait un autre facteur important à considérer si on veut rendre la personne physique propriétaire de ses données. Le vendeur ne sait pas du tout, ou alors très mal, combien valent ses données alors que l'acheteur, dont c'est le métier, connait parfaitement le prix sur le marché d'une *data* en fonction de l'information qu'elle véhicule. Il y a un énorme risque de déséquilibre. Les courtiers en données personnelles profiteront de la mauvaise information (ou de la naïveté) des vendeurs pour capter la plus grande partie de la valeur. On pourrait toutefois imaginer l'émergence de nouveaux intermédiaires, qui conseilleraient les individus *lambda* désireux de rentabiliser leurs *data*.[95]

Un nombre immense de données ne sont pas à proprement parler "personnelles". Elles se réfèrent aux caractéristiques d'au moins une seconde personne, que ce soit une connaissance, un autre membre de notre famille, etc. Serait-il dès lors vraiment légal et possible de vendre ces données sans lui demander son avis au préalable, sachant que cet individu pourrait subir un préjudice par ricochet lors de la cession de la donnée ? Le cas évoqué ici arriverait assez couramment en pratique, imaginons une personne décidant de vendre les données d'une discussion Facebook, il s'agit par hypothèse de données concernant au minimum une seconde personne.

95 F. MATTATIA et M. YAÏCHE, "Etre propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété? (Partie II)", *op. cit*., p. 43.

La propriété sur les données amènera également à un triple effet pervers tout en créant encore plus d'inégalités, parce que :

- cela poussera à mener toujours plus de transactions (beaucoup de personnes voudront échanger leurs informations numériques contre de l'argent),
- on aboutira à une accumulation des données par les entreprises en légitimant ce commerce par le marché alors que nous bénéficions pour l'instant d'une certaine protection en Europe en ce qui concerne les libertés et droits des individus,
- on augmentera les inégalités entre les plus pauvres, qui devront dévoiler leur vie privée pour obtenir un petit peu plus d'argent chaque mois, alors que les nantis pourront se payer le luxe de l'anonymat,[96]
- toutes les données ne valent pas le même montant et celles de certaines personnes sont beaucoup plus intéressantes (si vous êtes pauvre et un petit consommateur, vous n'intéresserez pas beaucoup les entreprises et collecteurs de données tandis qu'un milliardaire ou une célébrité sera plus courtisée).[97]

Et enfin, il y a selon nous un problème éthique dans le fait de vendre des biens qui pour l'instant font partie de la personne. Cet argument est peu, ou pas, abordé en doctrine alors qu'il nous semble primordial de rappeler que nos données et ce qu'elles disent de nous forment une part de notre identité.

Si les citoyens veulent réellement protéger leur vie privée, alors pourquoi ne pas utiliser des services qui le permettent déjà actuellement ? On peut imaginer le fait d'abandonner *Google Chrome* pour utiliser le réseau informatique décentralisé *Tor*, plus protecteur de notre vie privée, ou plus simplement en utilisant une majorité de service quotidien de manière anonyme.[98] Il faudrait pour cela que les individus se réveillent et comprennent qu'ils ont peu de prise actuellement sur le traitement de leurs *data*. Pour mettre en place une protection collective et effective de cette manière, il est impératif que chacun soit prêt à faire la démarche de protéger sa vie privée, ce qui n'est pas encore le cas.[99]

96 Y., PADOVA, "Entre patrimonialité et injonction au partage : la donnée écartelée? (Partie I)", *op. cit*., pp. 47-56.
97 G. MALGIERI et B. CUSTERS, *op. cit*., p. 300.
98 C. GATES et P. MATTHEWS, *op. cit*., p. 113.
99 *Ibidem*, p. 115.

Section 4 : L'Union européenne n'est pas compétente pour réglementer la propriété et la protection du RGPD

D'après les traités européens, et plus particulièrement selon l'article 345 du traité sur le fonctionnement de l'Union européenne (TFUE)[100], les autorités de l'Union n'ont pas le pouvoir de créer une propriété réelle sur les données. Les régimes de propriété sont en effet explicitement exclus des pouvoirs de l'UE selon l'article précité.[101] La seule solution serait de classer ce droit sur les données personnelles dans la catégorie des droits de la propriété intellectuelle car l'article 118 TFUE donne par contre le pouvoir aux autorités européennes de légiférer sur cette question. L'auteur faisant cette remarque, V. Janecek, n'est cependant pas convaincu que les *data* rentreraient dans la catégorie des droits de l'intellect pour autant. Il ne fait que remarquer que dans l'état actuel des choses, il s'agit de la seule solution.[102] Nous évoquerons plus tard la possibilité d'une consécration par un droit intellectuel, en attendant nous nous contenterons de faire remarquer que la Commission elle-même ne souhaite pas consacrer un "super droit de propriété intellectuelle" sur les données.[103]

Encore très récemment, une équipe de chercheurs a annoncé avoir développé un algorithme terrassant l'anonymat sur internet. [104] Il convient de prendre ce genre de nouvelles avec un certain esprit critique mais imaginons que ce soit vrai, à quoi correspondrait donc les données non-personnelles si la moindre activité sur le net permet de remonter jusqu'à nous et si les procédures d'anonymisation ne suffisent plus ? Le RGPD a déjà prévu cette éventualité d'évolution technologique dans son considérant 26 : les données non-personnelles qui perdent leur caractère anonyme à cause des avancées technologiques deviennent des données à caractère personnel.[105]

100 Traité de Lisbonne modifiant le traité sur l'Union européenne et le traité instituant la Communauté européenne, signé à Lisbonne le 13 décembre 2007, J.O.U.E, n°C 306.

101 V. JANECEK, "Ownership of personnal data in the internet of Things", *Computer Law & Security Review*, 2018, n°0, p. 11.

102 *Ibidem*, p. 12.

103 Règlement du 2018/1807 du parlement européen et du conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, *J.O.U.E.*, L 303, 28 novembre 2018, pp. 59-68 ; C. FLYNN, *op. cit.*, p. 34.

104 O. GUERGUINOV et E. WERY, "La donnée non-personnelle (anonyme) existe-elle ?", 1 aout 2019 sur *droit-technologie.org* (disponible depuis ce lien : https://www.droit-technologie.org/actualites/la-donnee-non-personnelle-anonyme-existe-elle/?fbclid=IwAR0J9JlhYy7-o1-Lk7ZXk7YBfPECfnmajO21WI9XGERvSeHypYNSm7jJR4I).

105 V. JANECEK, *op. cit*., p. 2.

Une question importante à régler serait également celle des usages ultérieurs à la cession des données. Comme nous aurions transféré nos données à un tiers, nous ne disposerions plus d'aucun contrôle sur son usage futur et son éventuelle revente à une entreprise qui nous déplairait fortement (plus aucun droit de regard ne nous serait ouvert). Cela signifierait donc au final d'être totalement dépossédé de tout contrôle sur l'usage de nos données.[106] Plutôt paradoxale comme constatation lorsqu'on se souvient de l'idée de départ, qui consistait à reprendre le contrôle de nos *data*. On voit ici par ce scénario à quel point le principe de finalité, imposé aux responsables de traitement par le RGPD, est important.

Et pour finir, il faut nuancer l'argument précédemment cité déclarant que l'instauration du droit de portabilité des données avec le RGPD était un premier pas vers un droit de propriété. Il est clair qu'il s'agit d'un renforcement du contrôle des individus sur leurs données et ainsi une forme d'appropriation, mais ce droit n'est ni absolu ni inconditionnel. Le rapporteur du RGPD et le Groupe de l'article 29 ont rappelé que la portabilité avait également pour objectif d'améliorer la mise en concurrence grâce au meilleur transfert des données des consommateurs. Le RGPD constitue donc un petit pas, certes, mais sa philosophie reste celle de la règlementation personnaliste centrée autour de la figure du *responsable de traitement*, personne envers qui les citoyens peuvent exercer leurs droits.[107]

## *Chapitre 4 : Ne peut-on pas imaginer un même résultat par une autre approche ? Quelles pourraient être ces autres solutions ?*

### Section 1 : Un nouveau droit intellectuel ou droit d'auteur

Dans cette première section, il sera question de transformer l'idée de la propriété privée "classique" sur la donnée en un nouveau droit intellectuel ou de se baser sur le droit d'auteur.[108] Il s'agit avant tout de voir si cette voie permet de gommer les défauts décrits ci-dessus.

106 Y. PADOVA, "Entre patrimonialité et injonction au partage : la donnée écartelée? (Partie I)", *op. cit*., p. 48.
107 *Ibidem*., pp. 51-52.
108 *Ibidem*, pp. 47-56 ; C. DESCHANEL, *op. cit*., p. 43 ; A. FLUECKIGER, "L'autodétermination en matière de donnée personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété?", *Pratique juridique actuelle*, 2013, vol. 22, n°6, pp. 837-864 (disponible en août 2019 sur : https://archive-ouverte.unige.ch/unige:30735 ) ; F. MATTATIA et M. YAÏCHE, "Etre propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété? (Partie I)", *op. cit*., pp. 63-65 ; V.-L. BENABOU et J. ROCHEFELD, *op. cit*., p. 106.

Les législateurs et de nombreux auteurs de doctrine sont forts hésitants en ce qui concerne la création de droits de propriété intellectuelle. Il est important de le rappeler, accepter une protection des créations de l'intellect n'a pas été une démarche évidente dans le passé.[109]

Un droit intellectuel sur la propriété des données pourrait être assimilé au droit d'auteur, il s'en rapproche en effet grandement. Les deux types de droits portent sur un objet immatériel, possèdent un droit moral également inhérent à la personne. On disposerait dans les deux cas d'un droit de divulgation, de paternité et d'intégrité sur l'œuvre. Le nouveau droit moral du propriétaire des données pourrait alors englober tous les droits qui découlent de l'actuelle autodétermination des individus et des prérogatives fournies par le RGPD (droit d'accès, droit à la rectification, droit à l'oubli). Il faudrait ensuite compléter cette liste préexistante avec des droits patrimoniaux qu'on pourrait librement négocier (droit d'utilisation pour des usages convenus contractuellement, droit de suite si cession ultérieure, etc.). Le cocontractant deviendrait alors un ayant-droit de la personne ayant consenti au traitement des données et serait libre d'utiliser et exercer les droits patrimoniaux, tandis que l'aspect moral de ce "droit d'auteur des données" resterait immuablement propriété de l'individu créateur de l'information.[110] En se basant sur le modèle des droits d'auteurs, ce nouveau propriétaire possèderait un contre-pouvoir qui améliorerait sa capacité à négocier.[111]

Si on veut par contre soumettre les données au droit d'auteur, il faudrait qu'elles remplissent plusieurs conditions. Il faudrait premièrement qu'elles soient reconnues comme des œuvres de l'esprit ; or bon nombre de *data* ne remplissent pas cette première condition. La deuxième caractéristique exigerait qu'elles puissent constituer une forme qualifiée d'originale et nouvelle. Si l'on suit la jurisprudence de l'arrêt *Infopaq* de la Cour de justice de l'Union européenne, il n'est pas possible de trouver beaucoup de données qui passeraient ce test avec succès.[112]

109 A. FLUECKIGER, *op. cit*., p. 861.
110 *Idem.*
111 *Ibidem*, p. 862.
112 F. MATTATIA et M. YAÏCHE, "Etre propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété? (Partie I)", *op. cit.*, p. 65 ; P. MOURON, *op. cit.*, p. 4 ; C.J.U.E., 16 juillet 2009, Infopaq International A/S contre Danske Dagblades Forening, C-5/08, ECLI:EU:C:2009:465.

La propriété d'une information, que Pierre Catala définissait comme étant *"tout message communicable à autrui par un moyen quelconque*",[113] est également contestée au point de vue de la théorie. Or, les réseaux numériques créent des données qui ne sont que des informations prenant une certaine forme. Cette forme de propriété pose en effet problème car énormément de juristes considèrent l'information comme étant "de libre parcours". Elle devrait donc pouvoir circuler sans entrave et ne pas faire l'objet de droits privatifs, ces constatations renvoyant d'ailleurs à de grandes libertés fondamentales comme la liberté d'information ou la liberté de parole. Certains envisagent néanmoins son appropriation et l'imaginent possible en pratique, si on réussissait à organiser son contrôle via des techniques contractuelles ou physiques restreignant son accès. Leur idée de départ étant que *"la notion de chose ou de bien est une représentation intellectuelle et que la qualité d'objet de droit peut être attribuée à un bien immatériel pourvu que ce bien soit considéré comme tel économiquement et qu'il soit digne de protection juridique"*. Ainsi, dès qu'un objet semble utile et appropriable, qu'il peut rentrer dans le commerce, il serait un bien et devrait être considéré comme tel.[114]

Cette solution aux problèmes de propriété privée des données ne semble pas être adéquate, qu'on la considère sous l'angle d'un nouveau droit intellectuel ou sous celui du droit d'auteur. Si un tel droit de propriété sur les données devait voir le jour, celui qui devrait en profiter serait certainement la personne qui aura regroupé les *data* en un ensemble cohérent, selon un certain *pattern* et une certaine logique. En effet, créer un ensemble cohérent est une démarche pouvant constituer un acte de création et se fondre dans la théorie classique du droit d'auteur. On récompense alors la personne créatrice d'un fichier reprenant l'ensemble des données, on ne confère absolument aucun droit à la personne physique créatrice de la donnée primaire. En instaurant un tel système, on se rapprocherait énormément du droit des bases de données (un droit *sui generis*). En reconnaissant un droit de propriété au producteur d'une base de données, on lui donne le pouvoir d'exiger que les tiers s'interdisent de reproduire cette collecte d'informations qui lui est propre. En légiférant ainsi, les autorités entendaient soutenir et avantager celui qui travaille à assembler des données. Il est compréhensible qu'une personne soit avantagée si elle produit un travail par rapport à ceux qui se contenteraient de copier-coller.[115] On ne défendrait donc pas les utilisateurs sur base de ce fondement légal, mais plutôt

113 P. CATALA, *Les transformations du droit par l'informatique. Emergence du droit de l'informatique*, Editions des Parques, 1983, p. 264.

114 V.-L. BENABOU et J. ROCHEFELD, *op. cit.*, p. 52.

115 Y. PADOVA, "Entre patrimonialité et injonction au partage : la donnée écartelée? (Partie I)", *op. cit.,* p. 53 ; F. MATTATIA et M. YAÏCHE, "Etre propriétaire de ses données personnelles : peut-on recourir aux régimes

les entreprises. Ce sont ces sociétés commerciales qui devraient alors profiter d'un tel droit d'auteur sur les données à caractère personnel collectées, mais celui-ci ne nous semble finalement pas pertinent, le système actuel des droits *sui generis* étant largement suffisant. Cette idée d'un droit intellectuel sur les données existe pourtant dans l'esprit d'auteurs de doctrines depuis très longtemps, comme nous le démontre un texte datant des années 1990 rédigé par Y. Poullet, reprenant déjà bon nombre d'arguments, toujours d'actualité, qui permettent de contredire ce projet.[116]

## Section 2 : La Directive secrets des affaires

L'introduction très récente de la directive "secret des affaires" (dont la loi de transposition vient d'entrer en vigueur au Luxembourg en juillet 2019) est une opportunité et alternative intéressante pour fonder un droit de propriété sur les données des entreprises. Il ne s'agit pas à proprement parler d'un droit de propriété en l'état, mais plutôt de l'octroi d'un intérêt à agir en justice. Pour bénéficier de ce droit il faut réunir quelques conditions assez simples déjà décrites en introduction, lorsque nous avons défini les données secrètes.

La protection des secrets permet d'assurer une sécurité juridique aux entrepreneurs dans leurs activités et a pour objectif d'améliorer la confiance lors d'échanges de données. Cette approche est également cohérente avec l'évolution de la jurisprudence française en matière de données, car celle-ci reconnaissait une propriété des données aux entreprises qui effectuent une collecte et un traitement de *data* (voir l'arrêt de la Cour de cassation française du 22 octobre 2014).[117] Dans cet arrêt, elle reconnait qu'un détournement de données peut être qualifié d'abus de confiance et donc implicitement que ces données constituent des biens de l'entreprise.[118]

traditionnels de propriété? (Partie I)", *op. cit.,* p. 65 ; M. KNOCKAERT et T. TOMBAL, *op. cit*.

116 Y. POULLET, "Le fondement du droit à la protection des données nominatives : « Propriétés ou Libertés »", *op. cit*., pp. 181-182.

117 Cass. crim. *française*, 22 oct. 2014, n°13-82.630**.**

118 Y. PADOVA, "Entre patrimonialité et injonction au partage : la donnée écartelée? (Partie I)", *op. cit.*, pp. 53-54.

Dans un autre arrêt de la Cour de cassation française, datant du 25 juin 2013[119], la chambre commerciale de la Cour décida qu'un fichier de clientèle n'est pas une chose rentrant dans le commerce qui nécessite une cession au moment du rachat de l'activité lorsqu'il n'y avait pas eu de déclaration préalable du fichier à la CNIL. Après lecture de cet arrêt et selon Y. Padova, il est possible de déduire *a contrario* que les données personnelles traitées et déclarées correctement sont susceptibles de faire l'objet d'un commerce ou d'être cédées librement par l'entreprise qui en fut le premier propriétaire.[120] Il s'agit ici de l'avis de l'auteur précité, nous ne sommes pas certains que l'on puisse être aussi catégorique dans une interprétation *a contrario* de ce genre. La Cour de Cassation refuse la qualification en premier lieu parce qu'il y avait infraction pénale (le défaut de déclaration du fichier à la CNIL), certes, mais sans autres éléments avancés par la Cour, il nous semble téméraire d'arriver si vite à une telle interprétation en cas de fichier légalement déclaré. Il est toutefois clair que dorénavant, grâce à la nouvelle directive, ce type de données sera nécessairement protégé, si on respecte les conditions pour pouvoir être qualifié de secret d'affaires. Cette avancée met donc un terme à cette relative incertitude.

Pour conclure, même si cette directive peut résoudre beaucoup de questions pratiques, lorsque nous arrivons à prouver que nos données doivent être qualifiées de secrets d'affaires ou de savoir-faire protégeables, jamais le droit en vigueur n'a permis de consacrer des droits de propriété sur l'information simple et ce n'est pas l'objectif de cette législation. La nouvelle Directive protège une catégorie définie d'information et il s'agit bien d'une exception au principe d'accès et de circulation des données.[121] Nos données personnelles classiques ne tomberont dès lors pas dans le champ d'application de cette législation et, malgré le souhait de certains auteurs, il faut chercher une base légale plus générale.

119 Cass. crim. *française*, 25 juin 2013, n°12-17.037.
120 Y. PADOVA, "Entre patrimonialité et injonction au partage : la donnée écartelée? (Partie I)", *op. cit.*, pp. 53-54 ; P. MOURON, *op. cit.*, p. 6.
121 S. GUTWIRTH et G. GONZALEZ FUSTER, *op. cit.*, p. 123.

Section 3 : Le droit à l'image

L'idée qu'on puisse être propriétaire d'une information qui concerne un individu remonte à John Lock et elle a permis *in fine* de faire évoluer la propriété classique vers la propriété intellectuelle. Ce type de propriété ne peut pas être la même que celle concernant des choses physiques. Il faut adapter les règles et pour cela A. Flueckiger propose de penser à un régime hybride entre celui des droits réels et celui des droits de la personnalité, empruntant aux deux.[122]

L'exemple du droit à l'image protégé soit par le droit d'auteur, soit par les droits de la personnalité et de la protection des données est une piste intéressante pour repenser la protection des données à travers le prisme de la propriété.

Le développement des droits de la personnalité est intimement lié à l'amélioration technologique des procédés de communication. En effet, le progrès a permis de matérialiser toujours plus d'informations émanant de la personnalité sur des supports physiques et le besoin de contrôler cette extension de notre personne s'est naturellement fait sentir. Ce fut ainsi très clairement le cas du droit à l'image. Ce droit naquit lorsque la photographie permit de rendre l'image d'un individu détachable, transportable et communicable à un large public. Les droits qui découlent de la personnalité sont donc exercés sur des objets extérieurs à la personne, plus ou moins tangibles et pouvant avoir une certaine valeur commerciale. Il est depuis lors possible d'exploiter son droit à l'image et de générer des revenus non négligeables, notamment lorsqu'on est une célébrité. Les droits de la personnalité sont et doivent rester dans la grande majorité des cas extrapatrimoniaux mais au travers de cet exemple, il nous semblait intéressant de rappeler qu'il a toujours existé une forme de patrimonialisation sous-jacente. Ce constat, même s'il ne peut servir de fondement à une patrimonialisation de nos données, est cependant riche en enseignements et arguments pour ses partisans.[123]

De grandes similitudes réunissent donc les droits des individus sur leurs données et leur droit à l'image. Ils sont tous deux nés grâce à l'évolution technologique et donc absents de la théorie classique de la propriété romaine. Ils se rapportent à un élément immatériel qui

122 A. FLUECKIGER, *op. cit*., pp. 859-861.
123 P. MOURON, *op. cit*., p. 4 ; C. DESCHANEL, *op. cit*., p. 36.

représente sans nul doute une part de l'identité de la personne concernée et ces deux prérogatives légales sont susceptibles de produire des revenus. Malgré ce parallèle assez intéressant, il semble néanmoins qu'à terme, la vision extrapatrimoniale soit encore la plus forte en Europe. L'image d'une personne ne constituant qu'une donnée personnelle parmi tant d'autres dans la masse du *big data*.

## Section 4 : Le patrimoine immatériel de données

Un auteur, T. Saint-Aubin[124], propose de sortir du débat sur l'opportunité d'un nouveau droit de propriété en utilisant une notion différente, celle de patrimoine immatériel. Ce concept beaucoup plus souple est selon lui plus adapté aux changements continus qui touchent les droits et obligations d'un responsable de traitement et semble particulièrement intéressant pour les entreprises.

Le patrimoine décrit dans cette section peut être défini comme "*l'ensemble des biens qui appartiennent à une personne physique ou morale. Le patrimoine inclut les droits et actions s'y rapportant. C'est l'enveloppe (fictive) qui a vocation à recueillir les droits, les biens et les obligations d'une personne. Il comporte un actif et un passif*".

Le point véritablement important dans le statut et la qualification juridique d'une donnée, c'est qu'elle peut être utilisée, enrichie et distribuée par son détenteur. L'exploitation est donc centrale mais sa valorisation est également primordiale. L'entreprise doit pouvoir déterminer la valeur des données dont elle dispose et pouvoir les inscrire, idéalement, dans l'actif immatériel de son bilan comptable. Ce qu'on appellerait donc *"patrimoine immatériel des données"* serait donc composé de biens spéciaux (les données) détenus par une société. Ces *data* pourraient donc être rattachées à plusieurs patrimoines en fonction des droits réciproques et des relations contractuelles entre les différents acteurs du marché de la donnée.[125]

124 T. SAINT-AUBIN, "Les nouveaux enjeux juridiques des données (big data, web sémantique et linked data)", *R.L.D.I.*, mars 2014, n°102, p. 99.
125 T. SAINT-AUBIN, *op. cit*., p. 99.

Cette notion étant moins sacralisée, elle pourrait avoir comme avantage de moins cristalliser le débat que la question de la propriété.[126] Il s'agit d'une idée qui reste néanmoins compliquée à mettre en œuvre et il nous semble difficile de valoriser correctement des données à un instant "t" dans un patrimoine. En effet, il est facile de dire ce que vaut une certaine quantité de données au moment d'une vente de données (à la suite d'une faillite par exemple, il faut liquider l'actif et la mise en vente du carnet d'adresse de la société Y vaut un montant X en euros) mais leur valeur peut beaucoup fluctuer dans le temps (si elles deviennent inexactes par exemple). De plus, cette proposition ne permet pas de répondre à notre souhait d'accorder davantage de droits aux particuliers, ce qui est le problème qui nous préoccupe.

126 *Ibidem*, pp. 99-101.

# Titre II : Le régime actuel basé sur la protection des libertés fondamentales

Il y a actuellement un consensus parmi la doctrine pour admettre que la marchandisation des données n'est pas équitable. Malgré tout on sent une forme de résignation de la population face au déséquilibre structurel qui existe dans la relation entre les *GAFAM* (principalement) et les individus. Les avis divergent quant à la réponse à apporter. Ici nous aborderons le scénario de la continuité du modèle se basant sur la nécessité d'un consentement des individus pour procéder à la collecte et au traitement de leurs données. Nous verrons également dans quelle mesure celui-ci peut encore nous protéger.[127]

## *Chapitre 1 : Histoire du régime actuel en Europe*

Dès le début des grandes révolutions du numérique, comme le lancement des premiers smartphones, des *Ipads* et autres tablettes ou le développement fulgurant des réseaux sociaux, l'Europe est restée très en retrait dans la course à l'innovation. Le fait d'être constamment à la traine lors des grandes révolutions numériques est une des causes de la longue période de dépendance technologique de l'Europe par rapport à ses concurrents commerciaux américains, chinois ou sud-coréens. L'Europe et ses pays membres, incapables de reprendre une initiative, n'ont plus exercés de maitrise sur les évènements, que ce soit du point de vue industriel ou réglementaire (le modèle anglo-saxon étant ultradominant dans ce domaine).[128]

A l'international, très peu d'Etats ont adopté une législation de protection des données comme l'Union européenne le fit le 24 octobre 1995 avec la directive 95/46/CE. Une grande majorité a préféré ne pas prendre part au mouvement impulsé par les décideurs européens, préférant se réfugier dans une position attentiste.[129] Les USA, à l'inverse, se réfugièrent dans des mesures d'autorégulation en grande partie chuchotées à l'oreille de l'administration

127 A. RALLET, *op. cit*., pp. 8-9.
128 LEROY, F., *Réseaux sociaux & Cie : le commerce des données personnelles*, Arles, Actes Sud, 2013, pp. 108-109.
129 *Ibidem*, pp. 83-84.

américaine par les milieux d'affaires.[130] Les formes de régulations et leur force de coercition divergent donc d'un pays à l'autre en fonction de l'implication des pouvoirs publics, de la culture juridique et de la puissance économique locale. Les Etats-Unis font moins appel à la réglementation que nous, préférant favoriser l'autorégulation. Ils s'appuient aussi plus facilement que nous sur les médias pour sanctionner un acteur qui dépasse les bornes, conscients du fait qu'une entreprise commerciale se doit de garder une bonne image.[131] Aux Etats-Unis, l'approche de la protection de la vie privée est également plus sectorielle, concentrée sur un type d'exploitation de données.[132]

C'est l'Europe qui se positionna dès le départ comme pionnière dans la protection de la vie privée en ligne. Une belle citation provenant d'une conférence de Berlin de 1989 nous le montre fort bien lorsque, peu de temps avant la chute du mur, les pays européens proclament que *" Nous ne voulons pas de l'Europe des marchands, nous voulons l'Europe des droits de l'homme".* La communauté européenne et ses commissaires à la protection des données décideront rapidement de privilégier la seconde option, ce qui explique pourquoi la protection des données est désormais une matière rattachée aux droits de l'homme en Europe.[133]

Le système actuel en UE est personnaliste, la protection de la vie privée est considérée comme un droit fondamental dans l'Union et est actuellement consacrée dans le droit communautaire par l'article 8 de la Charte des droits fondamentaux de l'Union européenne.[134] Certains auteurs comme Y. Poullet ont rapidement affirmé que si l'on admettait un droit de propriété ou un dérivé de celui-ci tel qu'un droit intellectuel sur les données, cela serait susceptible de constituer un danger. Un de ses arguments pour faire primer la thèse personnaliste était d'affirmer que cela conduirait à rendre la *privacy* négociable et susceptible d'achat à l'instar de n'importe quelle marchandise. Ce n'est pas l'existence de données nouvelles qui nécessitait l'instauration d'un droit au consentement mais bien l'évolution technologique de

130 *Ibidem*, p. 92.

131 A. RALLET et F. ROCHELANDET, "La régulation des données personnelles face au web relationnel : une voie sans issue ?", *Réseaux*, 2011/3, n°167, p. 26 (disponible en août 2019 sur : https://www.cairn.info/revue-reseaux-2011-3-page-17.htm).

132 *Ibidem*, p. 28.

133 CADOUX, L., "La protection des données personnelles en dehors de l'Europe communautaire", *Revue française d'administration publique*, janvier-mars 1999, n°89, p. 94.

134 Article 8 de la Charte des droits fondamentaux de l'Union européenne, adoptée le 7 décembre 2000 à Nice. :
*1. Toute personne a droit à la protection des données à caractère personnel la concernant.*
*2. Ces données doivent être traités loyalement, à des fins détermines et sur la base du consentement de la personne concerné ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux donnés collectés la concernant et d'en obtenir la rectification.*

l'époque qui créait alors de nouvelles formes de circulation de l'information. Ces nouveaux terrains de danger pour la vie privée devaient conduire à apporter des protections supplémentaires aux individus. C'est pour cela que le consentement libre et éclairé a déjà été préconisé à l'époque par les législations européennes en matière de données personnelles (comme dans le RGPD et son ancêtre la directive 95/46/CE).[135] Très incisif, Y. Poullet comprendra très tôt les enjeux d'une éventuelle mise en œuvre de la marchandisation de nos données comme le démontrent notamment ses propos en 1999. Il y défend le besoin d'une meilleure protection de nos *data* car "*Il s'agit d'une question de liberté, non pas d'une liberté aristocratique qui convient à quelques privilégiés désireux d'être laissés tranquilles, mais d'une liberté démocratique qui nous concerne tous, dans les relations sociales qui ont pris une nouvelle forme suite à la civilisation technologique*".[136]

L'information a une valeur économique, elle est donc la cible d'intérêts rivaux et concurrents. Actuellement la protection de la vie privée sur internet se fait en condamnant les auteurs de divulgations non consenties par les sujets. Il s'agit d'un mode de protection somme toute assez classique qui était déjà utilisé dans les atteintes à la vie privée par voie de presse par exemple (situation familiale, état de santé, etc.).[137]

## *Chapitre 2 : Point de vue allemand sur la protection des données personnelles*

Selon le *Grundgesetzt* allemande, l'individu a le droit de décider lui-même de la divulgation et de l'utilisation de ses données personnelles. A première vue, il s'agit donc d'une sorte de "pouvoir de disposition" de l'individu en ce qui concerne les *data* qui lui sont personnellement imputables et il peut ainsi toujours agir de la manière qui lui convient le mieux.[138]

135 Y. POULLET, "Le fondement du droit à la protection des données nominatives : « Propriétés ou Libertés », *op. cit*., pp. 185-186.
136 *Ibidem*, p. 186.
137 C. DE TERWANGNE, "Titre 5 – Droit à la vie privée : un droit sur l'information et un droit à l'information" in *Droit, normes et libertés dans le cybermonde*, Bruxelles, Éditions Larcier, 2018, pp. 556-557.
138 J.K.M. MÜLLER, "Dateneigentum in der vierten industriellen Revolution?", *Datenschutz und Datensicherheit*, 2019/3, p. 162.

Toutefois, cette forme de liberté est limitée. L'individu ne dispose pas d'un droit au sens d'une règle absolue et incontrôlable sur "ses" données, il est plutôt une personnalité qui se développe au sein de la communauté sociale et qui dépend de la communication. "L'information, même dans la mesure où elle est personnelle, représente une image de la réalité sociale qui ne peut être attribuée exclusivement à la personne concernée. La Loi fondamentale allemande a décidé de privilégier la communauté par rapport à l'individu. Cette restriction explique pourquoi leur Constitution ne prévoit pas de droit exclusif pour les données personnelles.[139]

Suivant cette logique, les données à caractère personnel ne peuvent donc pas relever d'un droit exclusif de *lege lata*. La propriété des données dans ce domaine pourrait entraîner des inégalités sociales et être préjudiciable à la société toute entière. Les données qui constitueront le *big data* ne peuvent être cédées aux tiers que de manière limitée et pour certaines finalités. Dans le cadre d'une utilisation coopérative des données générées, ce "nouvel or noir" de l'industrie moderne peut et doit encore être exploité dans le cadre de conventions relevant du droit des obligations, en respectant une exigence de consentement des individus. Un changement de cadre juridique en ce qui concerne les données non personnelles, n'est toutefois pas exclue pour l'avenir et même déjà en marche avec le Règlement *free flow of data*.[140]

L'analyse doctrinale allemande développée ci-dessus découle d'un arrêt très important de la Cour constitutionnelle allemande (le *Bundesverfassungsgerichtshof*).[141] Cet arrêt affirmait déjà en 1983, que « l'individu n'exerce pas une souveraineté absolue sur les faits le concernant, sa personnalité se développant au sein d'une communauté sociale, il ne peut vivre sans communiquer (...) c'est pourquoi en principe, l'individu doit accepter des restrictions de son "droit à l'autodétermination en matière d'information" et ce, en faveur de l'intérêt général prépondérant" ».[142]

139 *Ibidem*.
140 J.K.M. MÜLLER, *op. cit*., p. 166 ; A. FLUECKIGER, *op. cit*., p. 844 ; P. MOURON, *op. cit*., p. 8.
141 BVerfG., EUGRZ, 1983, 588.
142 Y. POULLET, "Le fondement du droit à la protection des données nominatives : « Propriétés ou Libertés »", *op. cit*., pp. 186-189.

## *Chapitre 3 : Les avantages et inconvénients du système actuel*

Section 1 : Les avantages apportés

La question est intéressante mais nous ne nous concentrerons pas sur ce point. Le but de ce travail est d'analyser ce qui peut être actuellement amélioré et de quelle manière répondre à ces problèmes. Il s'agira donc ici d'uniquement pointer les grandes lignes des points positifs de la protection des données européennes.

Au vu de l'ensemble des difficultés liées à une éventuelle propriété privée des données évoqué plus haut (titre I, chapitre 3), la conception extrapatrimoniale semble être préférable. Même si on peut obtenir des revenus qui découlent de droits de la personnalité comme le droit à l'image, *"la personne n'étant pas une chose, ses informations ne sauraient l'être non plus."*[143] Des intérêts comme la liberté d'expression, la liberté de conscience et le droit à l'autodétermination informationnel ne sauraient être évaluables en argent. Leur utilisation dans le commerce doit être la plus limitée possible pour ne pas tomber dans des excès tels que *Cambrigde Analytica* et son usage complètement dérégulé des données.[144]

Le RGPD précise bien dans son article 5 b) que les données à caractère personnel doivent être collectées pour des raisons spécifiques et spécifiées. Elles ne doivent pas ensuite subir de nouveau traitement incompatible avec cette première finalité.[145] Il s'agit d'une première défense qui semble préférable à ce que proposent les pro-propriétés, avec une telle législation il ne faut pas se demander si un individu a le droit d'agir pour protéger ses intérêts après la première cession de ses *data*. Ce principe peut cependant souvent être vu comme un obstacle à la recherche, au développement économique et à l'innovation.[146] C'est pourquoi le Groupe de travail article 29 a clarifié cet aspect de l'article 5 en détaillant ces deux aspects dans un avis.[147]

143 P. MOURON, *op. cit.*, p. 7.
144 *Ibidem*, pp. 7-8.
145 G. MALGIERI et P. DE HERT, "Making the most of new laws: reconciling big data innovation and personal data protection within and beyond the GDPR" in E Degrave, C de Terwangne, S Dusollier & R Queck (eds), *Law, Norms and Freedoms in Cyberspace - Droit, Norme et Libertés dans le Cybermonde: Liber Amicorum Yves Poullet.* 2018, Larcier, Bruxelles, p. 532.
146 *Ibidem,* p. 532.
147 WP 29, Opinion 03/2013 on porpose limitation, WP 203, 2 April 2013, pp. 11-20.

- Les données personnelles ne peuvent être collectées que dans des buts spécifiques, explicites et légitimes.
- Une nouvelle utilisation des données personnelles ne doit pas être incompatible avec leurs finalités. Lors d'un nouvel usage des données la finalité doit être définie avant ou au moment de leur collecte et non pas après.[148]

## Section 2 : Les inconvénients qui peuvent être améliorés

En Europe, les normes qui régissent la protection des données permettent d'exercer certains droits (comme obtenir une explication plus simple, la politique de confidentialité, permettre de corriger les données personnelles nous concernant, etc.). Ceci implique des coûts pour les exploitants, nécessite des formations de la part de leur personnel et la mise en place d'organismes chargés de surveiller la mise en œuvre de ces droits. Selon certains, ces dépenses élevées rendent limitée l'efficacité de cette méthode de régulation. De plus, il a été constaté par l'AFCDP[149] il y a plusieurs années que 82% des entreprises et administrations publiques françaises ne respectaient pas les obligations que leur imposait déjà la directive 95/46/CE. Le RGPD a sans doute amélioré ce pourcentage depuis lors grâce aux meilleures formations de prévention au sein des entreprises, la mise en place des DPO et les menaces d'amendes conséquentes qui existent dorénavant. Néanmoins, le chiffre de 82% reste éloquent, la protection de nos données et de la vie privée selon la vision UE n'est pas encore une culture qui va de soi dans certains des Etats-membres.[150]

De nouveau, la défense passive des individus face à la collecte de leur donnée est une vision qui n'est pas réaliste et est profondément inefficace. Il va falloir participer à créer une responsabilisation et une émancipation des citoyens *(active empowerment)*. Cela ne peut s'améliorer qu'à travers une prise de conscience du public de la valeur de leurs données, leur utilisation actuelle et des moyens de s'en prémunir.[151]

148 G. MALGIERI et P. DE HERT, *op. cit.,* p. 533.
149 L'Association Française des Correspondants à la Protection des Données à Caractère Personnel
150 A. RALLET et F. ROCHELANDET, *op. cit*., p. 33.
151 G. MALGIERI et P. DE HERT, *op. cit.,* p. 527.

C'est pourquoi il faut avant tout apprendre et expliquer les algorithmes aux citoyens. Actuellement ces programmes sont bien souvent inintelligibles. Les citoyens n'étant pas familiarisés avec des concepts tels que le *deep learning* utilisé lors de la création des services qu'ils utilisent quotidiennement. Parfois il arrive que le programmeur ou l'entreprise propriétaire de l'IA soit incapable de comprendre pourquoi la machine arrive à une conclusion plutôt qu'à une autre. Des exemples d'IA ayant échappés au contrôle de leur concepteur ne sont pas compliqués à trouver. On peut ainsi citer une intelligence artificielle de *Google* qui avait besoin de communiquer et interagir avec des internautes pour "mettre au point son intelligence".[152] Au bout d'une journée et par la faute d'individus mal intentionnés et déterminés, l'IA a fini par créer des tweets racistes et conspirationnistes sur base de son algorithme. *Google* a du couper le programme en urgence.[153] Il peut aussi arriver qu'elle se contente de reproduire les mêmes discriminations que l'être humain subit dans la vie de tous les jours. Une intelligence artificielle d'Amazon chargée d'analyser les éventuels recrutements a été entrainée à noter des CV principalement à l'aide de profils masculins, ce qui a amené l'IA à considérer les candidatures d'hommes systématiquement préférables à celles de femmes. Leurs profils furent constamment moins bien notés que leurs homologues masculins durant toute la mise en œuvre du projet uniquement parce que le mot *women* apparaissait dans leur CV. Cette erreur de programmation lors de la mise en place du logiciel a donc bien conduit à une discrimination claire en pratique.[154] Pour contrer tous ces potentiels effets, il est important qu'on puisse avoir le droit de demander une explication technique, qu'il y ait la possibilité d'offrir ladite explication et surtout de pouvoir contester le verdict découlant d'une intelligence artificielle si la décision risque d'être injuste ou injustifiée. Les machines, tout comme leur concepteur, ne sont pas infaillibles et il faut pouvoir garder un pouvoir de contrôle.[155]

---

152 Le programme devenait de plus en plus intelligent avec le temps et les nombreuses interactions qu'il avait avec la communauté de *Twitter*. Chacune des réponses humaines lui permettant d'affiner son "intelligence" artificielle et sa capacité à former des réponses censées. Il s'agit là d'un exemple d'apprentissage par *Deep Learning* évoqué en introduction.

153 M. TUAL, "A peine lancée, une intelligence artificielle de Microsoft dérape sur twitter", 24 mars 2016 sur *lemonde.fr* (disponible depuis ce lien : https://www.lemonde.fr/pixels/article/2016/03/24/a-peine-lancee-une-intelligence-artificielle-de-microsoft-derape-sur-twitter_4889661_4408996.html) ; E. LECOMTE, "L'IA de Microsoft est-elle réellement devenue raciste au contact des internautes ?", 25 mars 2016 sur *sciencesetavenir.fr* (disponible depuis ce lien : https://www.sciencesetavenir.fr/high-tech/intelligence-artificielle/l-ia-de-microsoft-est-elle-reellement-devenue-raciste-au-contact-des-internautes_31260). ; Il nous semble important de préciser que si l'expérience a si mal tourné, c'est en grande partie par la faute d'individus mal intentionnés ayant volontairement nourrit l'intelligence artificielle de messages négationnistes ou racistes. La principale erreur et faute des développeurs ici aura été d'avoir surestimé l'homme plutôt que sous-estimé la machine.

154 P. SIGNORET, "Amazon a du désactiver une IA qui discriminait les candidatures de femmes à l'embauche", 10 octobre 2018 sur *numerama.com* (disponible depuis ce lien : https://www.numerama.com/tech/426774-amazon-a-du-desactiver-une-ia-qui-discriminait-les-candidatures-de-femmes-a-lembauche.html).

155 G. MALGIERI et P. DE HERT, *op. cit*., p. 541.

L'approche actuelle de la protection des données ne permet pas de protéger les données des citoyens en tant qu'ensemble, en tant qu'atout économique, mais uniquement d'un point de vue personnel, émotionnel d'un individu.[156]

Dans notre monde ultra connecté et qui nous "dévoile" sans cesse, la notion de vie privée doit évoluer pour atteindre maintenant la maîtrise de chacun sur les informations et données qui le concernent personnellement. La vie privée ne se réduit pas à une recherche de la confidentialité mais aussi et surtout la maîtrise de son image informationnelle. Il faut qu'on ait accès aux données conservées/utilisées par des tiers et qu'on puisse connaître leur usage.[157]

Pour arriver à une parfaite maîtrise des données par les individus, il y a plusieurs principes et droits à mettre en place et à respecter. Tout d'abord, il faut garantir une forme de loyauté. La collecte et le traitement des *data* doivent se faire de manière transparente et sans tromperie. Ensuite, il faut que ledit traitement suive une ou des finalité(s) explicite(s) et légitime(s) tout en s'assurant que les données ne soient conservées que le temps nécessaire pour satisfaire la finalité de base. Et enfin les données doivent être de bonne qualité, c'est-à-dire exactes, précises et mises à jour. Grâce au droit de rectification des données incorrectes et au droit d'effacement des données non pertinentes par les individus, cela ne devrait pas être trop ardu de réclamer la maîtrise des données pour ce troisième point.[158]

156 *Ibidem*, p. 528.
157 C. DE TERWANGNE, *op. cit.*, p. 567.
158 *Ibidem*, pp. 567-568.

Si l'on a néanmoins perdu confiance dans la régulation actuelle et dans notre capacité de contrôler nos données, comment au minimum réussir à garder un semblant de contrôle sur notre personne numérique et la protéger des intérêts des tiers ? Il y a plusieurs stratégies conseillées :

- la clandestinité, pas de solution plus efficace qu'une non-existence totale sur les réseaux sociaux et la non-divulgation d'informations. C'est également la position la plus dure à tenir, dans notre société où une grande partie des pratiques sociales passent par l'interaction et l'exposition sur le net.
- la contre-information vise à manipuler les gestionnaires de données en ne divulguant que certaines informations, toujours à notre avantage. Une telle position sur internet est cependant assez difficile à tenir voire impossible.
- enfin, la multiplication des identités consiste dans le fait de diviser sa personne et son identité en plusieurs parties, une publique et l'autre privée. Publiquement, il est recommandé d'utiliser un pseudonyme (sur *Twitter* par exemple) et de n'y partager qu'un minimum d'information sous cette forme. La partie privée peut être composée d'éléments plus riches en informations personnelles lorsqu'on s'est assuré de l'avoir limitée à un cercle de connaissances restreint.[159]

Malgré tout cela, le cloisonnement des identités numériques est difficile à maintenir et de toute façon les algorithmes peuvent de mieux en mieux remonter jusqu'à notre identité réelle. Ces pistees sont donc toujours intéressants à suivre mais il ne faut pas trop donner de crédit à ce type de conseils afin de protéger sa sphère privée.[160]

## Section 3 : Les problèmes de ce modèle qui ne peuvent pas être résolus

Quand on demande à une personne physique son consentement préalable à la collecte de ses données à caractère personnel, il n'y a pour l'instant pas réellement d'alternative crédible.[161] Beaucoup de citoyens ne se posent donc même pas la question de s'ils vont lire les conditions d'utilisations du nouveau réseau social à la mode. De toute façon se disent-ils, "il est gratuit et je veux pouvoir y retrouver mes amis". On voit bien les limites du système basé sur le consentement. La réponse classique aux problèmes de protection de la vie privée sur internet

159 A. RALLET et F. ROCHELANDET, *op. cit.,* pp. 43-47.
160 *Ibidem*, p. 45.
161 A. FLUECKIGER, *op. cit*., p. 856.

a souvent été de renforcer les exigences de consentement. C'est ce qui s'est passé lorsque le RGPD entra en vigueur et que nous fûmes constamment harcelés de pop-up sur chaque site consulté, ceux-ci nous demandant (souvent erronément) de renouveler notre consentement. Pourtant poursuivre le renforcement du consentement des internautes ne permet pas forcément d'améliorer leur pouvoir de contrôle.[162]

Le RGPD incarne donc cette ambition de maintenir les individus dans une attitude réactive en matière de protection de leurs données. La notion de consentement défini à l'article 4, 11) du RGPD comme étant "*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*" est centrale dans cette conception non proactive.[163]

Il s'agit donc bien d'accepter. Le nouveau Règlement oblige les responsables de traitement à recueillir le consentement explicite des personnes physiques concernées et de cette façon il les transforme de facto en "machines à consentir". En pratique, aucun individu ne prend la peine de lire les interminables conditions d'utilisation et politiques de confidentialité. Tout cela a fini par conditionner le consommateur à cliquer compulsivement et machinalement sur un bouton "j'accepte". Nous arrivons alors à un paradoxe dans cette quête d'un libre arbitre qui dans les faits se matérialise par un geste compulsif. Plus on donne au consentement la garantie d'être éclairé en s'assurant plusieurs fois de sa sincérité, plus la réactivité et la réflexivité des personne physique diminue.[164]

La règlementation actuelle en Europe permet d'avoir un droit de regard sur l'usage qui est fait de nos données. Cependant, la multiplication des modes de collecte et de transmission des informations peut faire douter de la mise en œuvre pratique de telles mesures.[165]

162 *Ibidem*, p. 857.
163 A. RALLET, *op. cit*., p. 10. (nous soulignons dans le texte)
164 *Ibidem*.
165 A. RALLET et F. ROCHELANDET, *op. cit.,* p. 21.

Il est difficile, voire impossible, de promettre et garantir l'effacement de données personnelles. La règle légale doit faire face à de sérieux problèmes pratiques ; la non-rivalité des *data*, leur copie facile et peu couteuse, la persistance des données numériques ainsi que le contexte d'interactions décentralisées entre tous les internautes (où chacun peut détenir une *data* et la remettre en jeux après sa suppression.[166] De plus vouloir couper l'accès à une information peut rapidement déclencher un effet Streisand[167], surtout sur internet. Les internautes n'acceptant pas la mise en place de ce type de limitation participent alors activement à la faire circuler encore plus, alors que la donnée effacée aurait pu rester discrètement en ligne en l'absence d'action en justice.

Avec internet et nos moyens de télécommunications modernes, l'externalité est également devenue un problème. Il est par exemple possible de détecter avec plus ou moins de facilité l'émetteur de multiples messages de *spamming* mais il sera souvent difficile de le sanctionner. Celui-ci ayant de forte chance d'être protégé par différentes couches d'écrans fictifs. On peut très bien imaginer réussir à remonter jusqu'à l'adresse IP originelle tout en étant ensuite empêché d'agir en raison de l'extraterritorialité.[168]

Les législations sont généralement nationales ou européennes. Or les grands acteurs du web sont habituellement des multinationales ayant bâti et construit leurs activités au niveau international. Tant qu'aucune règle claire et ambitieuse n'existera au niveau international, il faudra dès lors faire face aux concurrences réglementaires, à l'extraterritorialité.

166 *Ibidem*, p. 40.

167 L'effet Streisand désigne le phénomène par lequel, le fait pour une entreprise ou une personne de vouloir faire cesser la diffusion d'une information (article, parodie, image,..) qui nuit à son image sur Internet se traduit le plus souvent par l'effet contraire à celui recherché, c'est à dire par une diffusion finalement plus large de l'information en cause.

Le nom d'effet Streisand vient du fait que la chanteuse Barbra Streisand a voulu faire cesser en 2003 la diffusion d'une photo aérienne de sa villa sur Internet en demandant notamment des dommages et intérêts astronomiques. Sa demande et l'écho qui lui a été fait ont finalement provoqué une diffusion beaucoup plus importante de la photo. ; B. BATHELOT, "Définition : Effet Streisand", 18 décembre 2018 sur *définitions-marketing.com* (disponible depuis ce lien : https://www.definitions-marketing.com/definition/effet-streisand/).

168 A. RALLET et F. ROCHELANDET, *op. cit.,* p. 24.

De plus si la réglementation nationale fixe des sanctions, elle s'appliquera avant tout aux exploitants indigènes, qui ont leur siège et activité principale sur le territoire de l'Etat en question. Attaquer et condamner une société étrangère est possible en cas d'application extraterritoriale (notamment dans le cas du RGPD, applicable notamment à partir du moment où un responsable de traitement ou un de ses sous-traitants a des activités sur le territoire européen).[169] Il ne faut cependant pas sous-estimer les retombées diplomatiques de ce genre d'outil juridique. Les français sont justement en train d'en faire les frais en créant leur toute nouvelle taxe GAFA. Le président Trump ayant déjà répondu qu'il allait surenchérir en taxant leur vin en retour[170]

## Section 4 : Le droit à l'information et son articulation avec la vie privée

Nous quittons ici de la question de la collecte et du traitement des données pour discuter de la possibilité d'utiliser des données personnelles lorsqu'il s'agit d'accomplir une mission d'information. En effet, certaines divulgations d'informations privées peuvent être légitimes s'il s'agit d'exercer sa liberté d'expression ou un droit à l'information du public, pour cela il faut pouvoir démontrer l'intérêt public de l'information. On ne peut pas non plus obliger les médias à prévenir au préalable la personne concernée lorsqu'une info la concernant est diffusée, ce serait courir le risque d'une forme de censure avant diffusion. Cependant, si la communication au public n'intervient pas dans le cas d'une information couverte par le droit du public à l'information il faut alors obtenir le consentement du concerné avant diffusion ou divulgation.[171]

169 *Ibidem* + Article 3 du RGPD :

1. *Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.*
2. *Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées :*
   a) *à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou*
   b) *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.*

170 LE SOIR, "« La stupidité de Macron » : Trump menace le vin français en réponse à la taxe GAFA", 27 juillet 2019 sur *lesoir.be* (disponible depuis ce lien : https://www.lesoir.be/238819/article/2019-07-27/la-stupidite-de-macron-trump-menace-le-vin-francais-en-reponse-la-taxe-gafa).

171 C. DE TERWANGNE, *op. cit.*, p. 558.

C'est dans le but de se protéger contre une société de surveillance (essentiellement étatique) que fut créé le principe de secret des lettres[172] (article 29 de la Constitution belge, modernisé ensuite en respect de la correspondance[173] pour devenir finalement confidentialité des communications[174]).[175] La confidentialité doit porter autant sur le message en lui-même que sur les données de communications (par exemple le nom de l'émetteur, sa location, la durée, l'adresse IP, etc.). La Cour de Justice de l'Union européenne refuse ainsi que l'on retienne toutes les données de communication de tous les citoyens durant une certaine période avec pour unique motif qu'elles pourraient être utiles en cas d'enquête criminelle les concernant. Elle a condamné cette conservation généralisée et indifférente de l'intérêt pratique des données dans deux arrêts[176], jugeant qu'on ne satisfaisait pas à l'exigence de proportionnalité dans la poursuite d'un objectif d'intérêt général. Elle laisse néanmoins aux Etats le droit de prévoir la conservation de données ciblées pour lutter contre la criminalité grave.[177]

Il y a tout de même une forme de paradoxe lorsqu'on confronte cette façon très juste de la cour de juger disproportionnée cette conservation systématique et massive de données par les États à la pratique des entreprises privées pionnières du numérique et de leurs services tels que *Messenger*, *Instagram* ou *Skype*. Ces dernières conservent dans le temps beaucoup d'informations sur leurs usagers pour améliorer leurs techniques de profilage de leurs clients.[178] Ce même profilage va ensuite pouvoir être utilisé à des fins politiques, grâce à des campagnes électorales reposant sur un marketing coûteux et gourmand en *data* dans lesquelles les réseaux sociaux privés jouent un rôle très important. La boucle est en quelque sorte bouclée, les politiciens utilisant les données récoltées par les *data brokers* pour se faire réélire par un moyen détourné.

172 Voy. not. art. 29 Const.
173 Not. art. 8 CEDH
174 Not. art. 7 de la Charte des Droits fondamentaux de l'Union européenne
175 C. DE TERWANGNE, *op. cit.*, p. 559.
176 C.J.U.E., 8 avril 2014, Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a., C-293/12, ECLI:EU:C:2014:238 ; C.J.U.E., 21 décembre 2016, Tele2 Sverige AB contre Post- och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a., C-203/15, ECLI:EU:C:2016:970.
177 C. DE TERWANGNE, *op. cit.*, p. 560.
178 C. DE TERWANGNE, *op. cit.*, p. 561.

## *Chapitre 4 : Le privacy by design, une bonne solution ?*

Qu'est-ce que le principe de la *privacy by design* (PbD) ? Il s'agit d'un *"mode de régulation séduisant puisqu'il intègre la protection des données à caractère personnel dès la conception des outils de collecte, de traitement ou d'exploitation des données*." Ce concept est donc censé agir comme un filtre qui minimise les risques d'exploitation contraire à la vie privée des utilisateurs du service.[179]

Il existe depuis le début des années 2000 mais les autorités européennes ont récemment décidé de consacrer le principe du *privacy by design* en le consacrant dans le RGPD à l'article 25. Un des grands intérêts du *privacy by design* est de faire peser la charge de la mise en œuvre d'une bonne régulation de la protection de la vie privée sur les opérateurs collectant les données. Elle doit permettre en théorie aux autorités de régulation nationales de mener une politique de responsabilisation des responsables de traitement tout en diffusant une culture de l'éthique des données.[180]

De nombreuses critiques sont cependant adressées aux techniques de *privacy by design*. Tout d'abord le fait de traduire en algorithmes ses principes très théoriques est un sacré défi, car leur effets pratiques sont généraux et flous. Il n'est pas évident non plus de définir si une mise en œuvre pratique d'une politique de protection des données privées répond aux caractéristiques de la *privacy by design* ou non. Comme énoncé dans les chapitres précédents, il est également dangereux de se reposer sur ce genre de technologies (ici émanant du principe précité) pour espérer bénéficier d'une bonne protection. Il restera quoi qu'il arrive très compliqué de contrôler le nombre de copies d'un type de données circulant pour l'instant sur Internet.[181]

179 P. PUCHERAL, A. RALLET, F. ROCHELANDET et C. ZOLYNSKI, "La privacy by design : une fausse bonne solution aux problèmes de protection des données personnelles soulevés par l'open data et les objets connectés ?", Victoire éditions, 2016/1, n°51, p. 90. (disponible en aout 2019 sur : https://hal.archives-ouvertes.fr/hal-01427983 ).

180 *Ibidem*, p. 92 ; A. RALLET, F. ROCHELANDET et C. ZOLYNSKI, "De la privacy by design à la privacy by using", *Réseaux*, 2015/1 (n°189), p. 17. (disponible en août 2019 sur https://www.cairn.info/revue-reseaux-2015-1-page-15.htm?contenu=article).

181 P. PUCHERAL, A. RALLET, F. ROCHELANDET et C. ZOLYNSKI, *op. cit*., pp. 96-97.

De plus, on peut se demander ce que vaut le principe de *privacy by design* dans le monde numérique construit justement sur la base du principe inverse, à savoir le fait de pousser les individus à partager leurs informations et à diffuser un maximum leurs données.[182] Ces principes sont bel et bien enseignés et mis en avant mais il s'avère qu'en pratique certains acteurs n'y font guère attention. Un des meilleurs moyens d'arriver à une *privacy by design* satisfaisante serait de développer une protection décentralisée des données, sur base d'un Cloud personnel par exemple.[183]

Que faire pour mieux se protéger alors ? De nouveau, il est argué que la solution doit venir des individus et d'une meilleure information/formation de chacun aux données. Ainsi, il serait possible de basculer vers une *privacy by using*. Il serait alors impératif que les sujets deviennent plus "actifs" dans la protection de leurs données par un mécanisme d'apprentissage. Il faut que les personnes physiques soient capables de comprendre les grands enjeux de la protection des données. Les problèmes principaux, déjà cités, sont l'asymétrie d'information entre les acteurs et les conséquences néfastes d'une surexploitation ou d'une diffusion de certains types de données.[184] On en revient donc de nouveau à la notion d'*empowerment* énoncée précédemment mais dans un autre contexte.[185]

182 A. RALLET, F. ROCHELANDET et C. ZOLYNSKI, *op. cit*., p. 25 ; I. RUBINSTEIN, *op. cit*., p. 1. *Ibidem*, p. 43.
183 *Ibidem*, p. 43.
184 *Ibidem*.
185 P. PUCHERAL, A. RALLET, F. ROCHELANDET et C. ZOLYNSKI, *op. cit*., pp. 98-99.

# Titre III : La donnée, bien commun.

## *Chapitre 1 : Le bien commun, réelle solution à nos problèmes ?*

Section 1 : Récapitulatif des constats actuels

La création artistique vit pour le moment un grand bouleversement et de grands changements grâce (ou à cause, c'est selon les points de vue) à la possibilité de numériser les œuvres et de les partager sur Internet. Ces créations sont devenues aisément duplicables, on peut les copier et conserver un exemplaire pour un cout très peu élevé (voir nul via le piratage) ce qui conduit à la "disparition de la rareté".[186] Les ayants droit ont donc de plus en plus de mal à défendre leur propriété. Pourtant les législateurs ne baissent pas les bras et multiplient les textes (HADOPI, ACTA, *Protect IP Act*, etc.) pour satisfaire les propriétaires originaux même si cette surenchère semble assez vaine. Le modèle de la propriété intellectuelle semble s'essouffler sur cette question et peine à se réinventer.[187] Cette solution ne semble pas si prometteuse que cela, impliquant peut-être d'imaginer quelque chose de nouveau…

La foule est créatrice sur internet, elle finance de petits projets indépendants via le *crowdfunding* et les plateformes de financement participatif comme *Tipeee*. On a ainsi pu se rendre compte grâce à *Youtube* et Wikipédia notamment que certains étaient prêts à fournir un travail sans appât du gain ni réels espoirs de retours sur investissement, mais en général simplement par passion.[188] Une partie des données présentes sur la toile sont créées par des internautes qui ont mis en commun leur ressources et leur travail (économie participative). Or il arrive qu'une grande partie de ces bénéfices soient récupérés par des agents économiques "classiques" complètement étrangers à l'idéologie de partage qui motivait et sous-entendait le projet initial. On constate donc une forme de paradoxe et cynisme dans ce "déplacement de valeur" à la lueur des résultats finaux. Une meilleure protection de la création commune pourrait-elle améliorer la situation ?[189]

186 V.-L. BENABOU et J. ROCHEFELD, *op. cit.,* p. 30.
187 *Ibidem*, pp. 48-51.
188 *Ibidem*, pp. 34-35.
189 V.-L. BENABOU et J. ROCHEFELD, *op. cit.,* p. 22.

Seuls les collectifs de citoyens ont le pouvoir de reconquérir un pouvoir de négociation effectif dans le procédé de valorisation de leurs données. Si les individus ne restent que des fournisseurs de données brutes et quasiment sans valeurs, ils ne seront jamais à même d'imposer leur choix à qui que ce soit dans ce marché. [190] Comme le rappelle P. Bellanger, "*L'individualisation juridique des données conduit à atomiser un droit collectif potentiel en une somme de droits privés plus facilement solubles : clic d'acceptation par clic d'acceptation. Il n'est d'ailleurs pas étonnant que les entreprises du réseau les plus dataphages défendent séparément ou conjointement ces deux thèses [privatisation ou non-réglementation des données] : elles leur ouvrent grandes les portes de la domination absolue*"[191]

Les réflexes actuels des législateurs consistent à renforcer et confirmer un droit exclusif personnel sur ses propres données, que ce soit par la consécration d'un droit au transfert de ses données personnelles, à leurs modifications ou leurs destructions. Même si cette vision comporte un certain nombre d'avantages, peut-on vraiment affirmer qu'elle représente bien la réalité des données aujourd'hui ?[192]

L'individualisation juridique des *data* conduit donc à une atomisation d'un droit collectif en une somme de droits privés et personnels dont il est plus facile de s'affranchir, par une simple demande de consentement en ligne par exemple.[193] Nous allons voir ensemble dans les sections suivantes que tirer de ces constats et quel autre système P. Bellanger, A. Rallet et biens d'autres nous invitent à réfléchir.

190 A. RALLET, *op. cit.,* p. 16.

191 P. BELLANGER, Principes et pratiques des données personnelles en réseau, Contribution à l'étude 2014 du Conseil d'Etat : technologies numériques et libertés et droits fondamentaux, 2014 ; F. MATTATIA et M. YAÏCHE, "Etre propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété? (Partie II)", *op. cit*., p. 44.

192 P. BELLANGER, "Les données personnelles : une question de souveraineté", *Le Débat*, 2015/1, n°183, p. 15. (disponible en aout 2019 sur : https://www.cairn.info/revue-le-debat-2015-1-page-14.htm?contenu=resume).

193 *Ibidem*, p. 20.

Section 2 : Le commun, une réalité

Selon Pierre Bellanger (que nous rejoignons) les données sont actuellement organisées en réseaux, une totalité indissociable. Pour cela il avance plusieurs arguments :

- Les données à caractère personnel ne sont pas isolables en pratique. Diffuser ses photos, son agenda, son adresse, engage de facto les informations personnelles d'autrui sur lesquelles nous ne disposons d'aucun droit.
- Les données personnelles renseignent sur d'autres personnes. Grâce à des algorithmes de corrélation, une information me concernant peut, mêlée parmi celles d'autres individus, conduire à une information déduite par probabilité et prédiction des IA. Chacune de mes données renseigne indirectement sur mon voisin.
- Les données constituent une extension de notre personne. Il nous semble donc moralement incorrect et mauvais de "vendre" les données d'autrui contre un service.
- Le contrôle individuel de ses *data* par accord conventionnel de gré à gré devient impossible. Les collecteurs et *data brokers* sont destinés à voir leur nombre augmenter, ainsi que leur captation de données. Les contrôler ne sera plus possible en pratique, qui plus est à travers les divers exemples de rachats de données sur ce marché secondaire (évoqué au chapitre 1).
- La création d'un monopole des données est une réalité. La valeur d'une donnée augmente lorsqu'elle peut être replacée dans un contexte, lorsqu'elle est reliée à d'autres *data* pertinentes. Ainsi, il n'y a pas de valeur pour une donnée unitaire et les seuls pouvant dicter le marché sont les gros détenteurs de données.

Les données à caractère personnel se déterminent et s'influencent donc mutuellement et constituent un réel réseau.[194]

Comment qualifier juridiquement ce réseau de données ? Pour P. Bellanger, il s'agit *"d'un objet sur lequel toutes les personnes (...) disposent de droits, mais qui ne peut être matériellement divisé entre eux. Il n'est ni dissociable ni individualisable par nature, car chaque donnée personnelle renseigne sur les autres."* [195] Cela crée donc une forme d'indivision, une masse qui nous concerne tous. Cette impossibilité à séparer cet amas de données et son utilité collective devrait nous pousser à en faire un bien commun. Une *res communis*, que

194 P. BELLANGER, "Les données personnelles : une question de souveraineté", *op. cit*., pp. 16-17 ; A. RALLET, *op. cit.,* p. 16.
195 *Ibidem*, p. 18.

l'auteur décrit comme *"un bien qui appartient à tous mais qui ne peut appartenir à personne en particulier"* (article 714 du Code civil belge et français).[196]

Elinor Omstrom, prix Nobel d'économie, a montré qu'il pouvait exister des ressources gérées efficacement en communautés d'individus en sortant de la logique de marché ou de régulation étatique forte. Elle préfère le terme de "commun" plutôt que celle de bien commun car il s'agit en réalité d'une double nature. Un commun étant à la fois un type de bien (ressources pouvant être mises en commun dans un groupe) et une manière de gérer ladite ressource (une forme spéciale de gouvernance, de gestion).[197] De plus, pour elle, il n'y a pas de règles prédéfinies ou de modèle général pour gérer efficacement le commun, le collectif se doit de prendre lui-même les règles les plus pertinentes selon la situation précise.

## Section 3 : Proposition de réformes et prospections

Grâce à la constitution d'un commun, tout le monde pourrait avoir une possibilité d'agir pour protéger ses droits (retrait, opposition, transfert des données ou droit à l'oubli) sur ses propres données qui composent la masse à partir du moment où ses revendications ne mettent pas en danger les droits d'autrui. L'exercice des droits collectifs qui résulteront de cette mise en commun devrait de leur côté revenir à une autorité publique qui agirait dans l'intérêt général. Actuellement la meilleure solution serait certainement de confier ce pouvoir aux autorités de protection des données nationales (ex la CNIL en France), même s'il faudrait alors un bon nombre de réformes.[198]

La compétition en matière de données à caractère personnel doit se faire sur leur usage en pratique et non sur leur appropriation massive par les acteurs économiques. Les entreprises se doivent de créer de meilleurs services, plus efficaces pour battre leurs concurrents sur leurs marchés respectifs. Pour cela, ils pourront agir en utilisant une même base de données

196 *Ibidem*, p. 18.
197 A. RALLET, *op. cit.,* p. 16.
198 P. BELLANGER, "Les données personnelles : une question de souveraineté", *op. cit*., p. 18 ; A. RALLET, *op. cit.,* p. 17 ; D. BOURCIER et P. DE FILLIPI, "Vers un droit collectif sur les données de santé", *Revue de droit sanitaire et social*, Sirey, Dalloz, 2018, 2018 (3), p. 0 (disponible en aout 2019 sur : https://hal.archives-ouvertes.fr/hal-01850925/).

réglementée mais ouverte à tous, en tirer un maximum de valeur tout en permettant une compétition plus saine et équitable.[199]

En recourant à ce système inexistant à l'heure actuelle, on refuse la monétisation individuelle comme évoquée dans le chapitre 1 et également l'échange implicite "donnée contre service" du chapitre 2, inéquitable dans les faits. Dans le cas d'une donnée en tant que bien commun, il ne s'agit plus de "marché" mais de la mise en place d'un lieu de négociation collective entre un acteur agissant pour le bien commun, ses membres (simples citoyens), et des exploitants de données (entreprises, chercheurs, etc.) qui devront démontrer une finalité précise au traitement pour obtenir le précieux accès aux données. La contrepartie qui serait accordée aux individus par la mise en commun ne serait pas aussi directe qu'un montant d'argent dérisoire. Le but serait de négocier dans un intérêt qui procurerait des avantages collectifs aux membres sans rétribution monétaire directe. L'excédent, qui ne financera pas le fonctionnement pratique du commun, étant utilisé pour investir dans la recherche et les nouvelles ressources.[200] Pour financer ce système, pourquoi ne pas créer un système fonctionnant de la même manière que la SACEM pour le droit d'auteur ? [201] Les acheteurs de données personnelles devraient s'acquitter d'un forfait auprès de l'organisme collectif gestionnaire des *data* pour pouvoir accéder à un certain type de données, pendant un certain temps et selon une finalité bien précise.

## *Chapitre 2 : L'expérimentation de ce concept dans le domaine de la santé*

Le *Big data* est un ensemble d'informations qui constitue un outil très séduisant, son utilisation par l'intelligence artificielle permet d'imaginer des usages toujours plus sophistiqués. L'exploitation des données et leur analyse à grande échelle ne pourra aller qu'en s'accroissant. Il s'agit d'un potentiel de recherche et d'innovation énorme, notamment en matière médicale : il permet d'espérer des avancées dans la lutte contre le cancer, les maladies neurologiques ou les maladies orphelines (qui souffrent actuellement d'un manque de *data*).[202]

199 P. BELLANGER, "Les données personnelles : une question de souveraineté", *op. cit*., p. 20.
200 A. RALLET, *op. cit.,* p. 19.
201 A. RALLET, *op. cit.*
202 B. BÉVIÈRE-BOYER, "Données massives en santé : ébauche d'un droit prospectif", dans *Innovation en santé publique des données personnelles aux données massives (big data),* Paris, Librairie générale de droit et de jurisprudence, 2018, pp. 94-95.

Les données brutes, "matière première numérique" ne disposent actuellement pas de statut juridique spécifique unanimement accepté au niveau international. Elles pourraient donc être sujettes en pratique à un droit d'appropriation par des entreprises du secteur privé. Comme nous allons le voir, en matière de recherche, cela risque de remettre en cause leur utilisation dans un but collectif et dans l'intérêt général. Pour B. Bévière-Boyer, il faudrait conserver cette accessibilité à tous grâce à un statut juridique spécifique et novateur au bénéfice de l'ensemble des acteurs du secteur, quelle que soit leur origine.[203]

L'intelligence artificielle a conduit à un changement de mentalité dans un monde de la santé, déjà en profonde mutation. La mesure phare des nouvelles transformations, la médecine personnalisée, est très gourmande en *data*. Elle permettrait d'imaginer un suivi tout le long de notre existence, d'agir par prévention plus facilement et rapidement et pourrait conduire à l'amélioration des chances de détection des anomalies, voire permettrait des traitements sur mesure en prenant en compte toute une série de paramètres personnels.[204]

Les données recueillies en relation avec la médecine sont colossales. Aux USA, le système de santé aurait ainsi créé plus de 150 milliards de milliards d'octets de données. Jusqu'ici ces *data* brutes n'étaient pas ou peu exploitées mais grâce aux nouvelles méthodes de traitement des données, elles constituent dorénavant une richesse énorme pour l'innovation en matière de santé.[205]

Le RGPD considère comme données à caractère personnel touchant à la santé non seulement les informations concernant directement l'état de santé des individus mais également celles n'ayant qu'un lien indirect avec la maladie, telles les données d'usagers du système de santé (voir les considérants 35, 53 et l'article 4, 15) du RGPD[206]). Cette définition connait ainsi les mêmes délimitations que celle adoptée par l'OMS.[207]

203 B. BÉVIÈRE-BOYER, *op. cit*., p. 95.
204 *Ibidem*, p. 96.
205 *Ibidem*, p. 97.
206 *La définition exacte inscrite à l'article 4, 15) énonçant précisément que doivent être considérée comme données de santé : "les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne*"
207 M. MICHOT-CASBAS et C. HERVÉ, *op. cit*., p. 6.

Nous pouvons par exemple citer *IBM Watson* comme nouveau programme d'intelligence artificiel utilisant le *big data* dans le médical. Il pose des diagnostics dans le domaine de l'oncologie, en analysant et traitant les données à caractère personnel d'un patient, qu'il croise avec une base de données composée de milliers d'articles scientifiques. Certains programmes d'IBM peuvent également (en application de techniques de *deep learning* classiques déjà décrites supra) déterminer si un patient souffre d'un cancer de la peau ou non, et cela avec des taux de réussite très intéressants, plus élevés que celui de dermatologues professionnels (95% de bons diagnostics).[208]

De son côté, Google a mis sur pied une IA baptisé LYNA capable de détecter les cancers du sein dans 99% des cas[209] et a créé *Google Cloud for Healthcare* dont l'objectif est d'organiser l'information médicale mondiale et de la rendre accessible et utile. "Cette plateforme spécifique aux soins de santé implique l'utilisation de standards ouverts pour permettre le partage de données et la collaboration interactive entre les chercheurs tout en fournissant une plateforme sécurisée".[210]

On le voit, ce sont donc les *GAFAM* et autres géants du numérique qui souhaitent se positionner au mieux dans cette course à la *data* médicale. Ils sont actuellement détenteurs d'une quantité énorme de ce type de données alors que leur tactique actuelle consiste à ne revendiquer aucun privilège sur ce type de données et à les laisser en *open access*. Ces acteurs se contentent de continuer à amasser un maximum de données personnelles par le biais des collectivités, incitées par cette politique à faire confiance aux multinationales. Ils se sont rendus omniprésents et cela risque de poser à l'avenir des problèmes d'accessibilité directe des données s'ils venaient à changer d'avis et à limiter cet *open access*. Ces sociétés se placent actuellement dans une situation de quasi-monopole dans cette branche du *big data*.[211]

208 SCIENCES ET AVENIR et AFP, "Une intelligence artificielle capable de reconnaitre le mélanome avec 95% d'efficacité", 29 mai 2018 sur *sciencesetavenir.fr* (disponible depuis ce lien : https://www.sciencesetavenir.fr/sante/dermato/cancer-de-la-peau-une-intelligence-artificielle-meilleure-dans-le-depistage-que-les-dermatologues_124423) ; B. BÉVIÈRE-BOYER, *op. cit.*, p. 98.

209 V. CIMINO, "Google détecte le cancer du sein métastatique avec une précision de 99%", 15 octobre 2018 sur *siecledigital.fr* (disponible depuis ce lien : https://siecledigital.fr/2018/10/15/une-ia-by-google-detecte-le-cancer-avec-une-precision-de-99/).

210 (Propos de Gregory J. Moore, vice-président des soins de santé *Google Cloud* le 5 mars 2018 ; B. BÉVIÈRE-BOYER, *op. cit.*, p. 98.

211 B. BÉVIÈRE-BOYER, *op. cit.,* pp. 100-101.

Peut-on vraiment avoir confiance et penser qu'ils agissent dans des buts uniquement philanthropiques ? Leur intérêt est-il vraiment orienté vers l'intérêt des patients uniquement ou, comme pour *Facebook* par exemple, s'agit-il d'avancer dans le domaine de l'IA avec l'aide de chercheurs publics à moindre coût tout en bénéficiant, comme en France, de crédits d'impôt recherche ? Le risque majeur serait atteint si les *GAFAM* arrivaient à créer une situation de monopole complet concernant les données médicales.[212] Il s'agit pour B. Bévière-Boyer d'une question sous-estimée à l'heure actuelle en Europe.

Comme la collecte et l'exploitation des *data* s'effectue au niveau mondial, il ferait sens d'édicter de nouvelles normes internationales. L'auteur propose ici que les données anonymisées de santé soient considérées comme patrimoine commun de l'humanité ou comme un « bien commun ». Cela permettrait d'assurer leur accès à tous, à la différence d'autres types de données utilisées par les multinationales ayant un impact moins crucial sur la société entière. Il faudrait de plus prévoir que ce type de données, lorsqu'elles sont collectées massivement, soient obligatoirement stockées sur des serveurs n'appartenant pas aux *GAFAM*.[213]

La tendance actuelle consistant plutôt à sanctionner les géants du numérique dans leur tentative d'hégémonie et de destruction de toute concurrence[214], on peut espérer qu'une volonté politique finisse par émerger, sachant qu'une coordination au niveau mondial semble extrêmement compliquée. Les pays européens devraient au moins commencer par développer et favoriser les alternatives européennes ou nationales aux géants de la Silicon Valley, en les incitant à être plus respectueuses des règles communautaires (comme *Qwant* en France ou *DuckDuckGo* qui s'engagent à respecter la vie privée et ne pas récolter nos données personnelles).[215]

212 *Ibidem*, pp. 102-103.
213 *Ibidem*, pp. 107-108.
214 Dans un contexte complètement différent, voir l'amende infligée récemment à Google pour infraction aux dispositions du RGPD : J. LAUSSON, "La CNIL inflige à Google une amende record de 50 millions d'euros pour violation du RGPD", 21 janvier 2019 sur *numerama.fr* (disponible depuis ce lien : https://www.numerama.com/politique/457010-la-cnil-inflige-a-google-une-amende-record-de-50-millions-deuros-pour-violation-du-rgpd.html).
215 B. BÉVIÈRE-BOYER, *op. cit*., pp. 107-108.

Le droit à la vie privée ne devrait plus être perçu comme un droit uniquement personnel et individuel mais également comme un droit collectif, un droit qui appartient à un individu mais qui pourrait être exercé de manière collective par la communauté.[216] On se rapproche ici beaucoup de l'interprétation de l'autonomie défendue par la Cour constitutionnelle allemande dans l'arrêt précité. Et cela est logique lorsqu'on comprend qu'il est de plus en plus compliqué d'affirmer qu'une donnée est réellement "personnelle". Désormais celles-ci forment un réseau interdépendant et interconnecté.

Dans la mesure où un individu qui autorise une collecte ou traitement de ses données expose souvent - volontairement ou involontairement - la vie privée d'autres individus (violant ainsi leurs droits), il serait souhaitable d'avoir une vision plus collective de la protection des *data* et de la vie privée.

Introduire un nouveau droit de propriété n'apparaît dès lors pas pertinent dans le sens où il se rapporterait à un "bien" qui n'appartiendrait à personne et à tout le monde en même temps. C'est pourquoi nous militons en faveur d'une thèse qui considère les données en réseaux comme "bien commun" et qui confierait cette mission de protection de l'intérêt général à un pouvoir étatique indépendant[217] ou à un organisme neutre et indépendant.

Pour une auteure comme Julie Cohen (*"Turning Privacy Inside Out"*) il conviendrait que l'Etat soit responsable et puisse garantir une protection efficiente et efficace de la vie privée. Nous sommes d'avis que débuter cette expérience du bien commun en partant des données médicales est une très bonne idée.[218] Pour notre part, nous ne sommes pas sûrs que confier à l'État cette tâche extrêmement importante soit une très sage décision. Un organisme neutre et indépendant soumis à une série de contre-pouvoir et à une surveillance semble plus cohérent, au vu de l'immense pouvoir qui lui serait confié.

Nous pouvons en outre rejoindre des auteurs comme Pierre Bellanger ou Julie Cohen en affirmant qu'il est nécessaire de choisir une position collective sur nos données, limitant *de facto* certaines libertés individuelles au nom de l'intérêt général et du bien commun.

216 D. BOURCIER et P. DE FILLIPI, *op. cit*., pp. 12-13.
217 *Ibidem*, p. 1 et 13-14.
218 *Ibidem*, p. 14.

# Conclusion

Comme nous avons pu nous en rendre compte, les données personnelles sont toujours sujettes à de nombreuses interrogations en doctrine. Bon nombre d'entre elles n'ont d'ailleurs pas pu être abordées dans cette contribution malgré leur intérêt. A titre d'exemple, que deviendront les données à caractère personnel des européens traitées par des entreprises britanniques ? Si on aboutit à un *hard Brexit*, tout transfert de données sera illégal jusqu'à signature d'un accord de transfert de données entre l'Union européenne et le Royaume-Uni.[219] En ce qui concerne le traitement des données, un tout récent arrêt de la Cour de Justice de l'Union européenne vient apporter une nouvelle pierre à l'édifice mis sur pied par le RGPD.[220] La Cour a décidé à l'occasion de l'arrêt *Fashion ID* qu'un gestionnaire de site internet muni d'une possibilité de « *liker* » avec son compte *Facebook* peut être tenu (co)responsable avec *Facebook* de la collecte et du traitement des données récoltées.

Les données et plus généralement les droits du numérique sont assez neufs et demandent constamment de nouvelles réponses dans un édifice se construisant petit à petit. Cette évolution du droit des nouvelles technologies est en constante mutation parce qu'elle dépend d'avancées technologiques qui ont bouleversé notre quotidien à plusieurs reprises. Toutefois, ces droits concernent des questions assez classiques pour un juriste (la protection de la vie privée et des droits fondamentaux, la question de la protection des biens, de la propriété intellectuelle, etc.) transposées dans un nouveau cadre. Et il n'y a selon nous pas de raison de modifier dans ce nouvel environnement nos solutions juridiques qui découlent de choix de société, de notre histoire et d'années d'évolutions de la jurisprudence européenne et nationale.

219 LEMPÉRIÈRE, M., "Les transferts de données vers le Royaume-Uni après le Brexit", *Expertise*, avril 2019, pp. 139-140.

220 C.J.U.E., 29 juillet 2019, Fashion ID GmbH & Co.KG contre Verbraucherzentrale NRW eV, C-40/17, ECLI:EU:C:2019:629. + B. SALOVIC, T. LEONARD, E. WERY, "Bouton « j'aime » de Facebook : voici le verdict final de la CJUE", 29 juillet 2019 sur droit-technologie.fr (disponible depuis ce lien : https://www.droit-technologie.org/actualites/bouton-jaime-de-facebook-voici-le-verdict-final-de-la-cjue/).

Selon nous, et pour reprendre la formulation d'Isabelle Falque-Perrotin, la propriété privée des données est une "mauvaise bonne idée", très tentante de prime abord mais qui ne résiste pas à une analyse plus approfondie. Si une solution doit être trouvée, il est nettement plus intéressant d'élaborer des solutions à partir de droits existants comme le droit à l'image. C'est pour cela que la philosophie présidant au système actuel nous semble être une meilleure solution : protéger nos données en tant que partie de notre identité, en tant qu'éléments extrapatrimoniaux sur lesquels nous ne pourrons jamais perdre nos droits, nous semble préférable. Il faut cependant reconnaitre que notre protection actuelle n'est pas très effective. Dans les faits, il est de plus en plus difficile d'obtenir un consentement réellement éclairé et décidé de la part des internautes. Quelle autre solution mettre en place alors ? Tout d'abord, il faudrait responsabiliser les personnes par rapport à l'usage de leurs données. Informer le public et mieux l'orienter vers des services plus respectueux de la vie privée devraient être une priorité.

Ensuite, pour redistribuer un peu plus équitablement le revenu de l'exploitation des données, nous préconiserions de mettre en place un nouveau principe du *"prédateur payeur"* qui concernerait les entreprises les plus gourmandes en données à caractère personnel. La France s'est lancée dans une voie similaire par l'adoption d'une loi taxant les grandes entreprises du numérique mais elle est isolée internationalement. Amazon ayant déjà annoncé que cette taxe serait répercutée aux sous-traitants français, cette mesure risque d'être inefficace. Le principe de *privacy by design* pourrait-il nous permettre d'atteindre une meilleure protection ? Selon nous la réponse est négative, il s'agit sans nul doute d'un beau principe théorique mais trop peu utilisé et mis en œuvre en pratique par les acteurs les plus imposants. Il semble donc condamné à rester un symbole et un vœu pieux pour les acteurs du numérique.

Pour conclure, nous sommes d'avis qu'un meilleur avenir pour la protection et la valorisation de nos données passerait par la création d'un nouveau droit sur les données, considérées comme bien commun. Une gestion collective serait la plus à même de rééquilibrer la balance entre les citoyens et les géants du numérique. De plus la valeur de nos données, très faible lorsqu'elle est prise individuellement mais précieuse quand elle constitue une masse, en profiterait grandement. Il pourrait également s'agir là d'une solution pour rattraper les problèmes de dépendance et retard de l'Europe vis à vis des *GAFAM* et *BATX*, lutter contre le monopole des USA en IA tout en favorisant la recherche et les entreprises européennes. Récemment, en aout 2019, Google proposait aux passants d'une rue commerçante de racheter

leur visage pour 5$[221], les éléments principaux de nos identités valent-ils réellement aussi peu d'argent et s'agit-il vraiment de la société que nous voulons créer pour notre futur ? *Génération Libre* vous répondra sans doute par l'affirmative mais les défenseurs des libertés fondamentales certainement par un non catégorique.

221 C. MATYSZCZYK, "Google bought my friend's face for $5", 21 juillet 2019 sur zdnet.com (disponible depuis ce lien : https://www.zdnet.com/article/google-bought-my-friends-face-for-5/).

# *Bibliographie*

## Législations européennes

Convention européenne 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, 3 septembre 1953.

Charte des droits fondamentaux de l'Union européenne, adoptée le 7 décembre 2000 à Nice.

Traité de Lisbonne modifiant le traité sur l'Union européenne et le traité instituant la Communauté européenne, signé à Lisbonne le 13 décembre 2007, J.O.U.E, n°C 306.

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

Règlement du 2018/1807 du parlement européen et du conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, *J.O.U.E.*, L 303, 28 novembre 2018, pp. 59-68.

Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données, *J.O.U.E.*, L 281, 23 novembre 1995, pp. 31-50.

Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, *J.O.U.E.*, L 157, 15 juin 2016, pp. 1-18.

WP 29, Opinion 03/2013 on porpose limitation, WP 203, 2 April 2013, pp. 11-20.

Avis 7/2017 du C.E.D.P. sur la proposition de règlement relatif à la vie privée et aux communications électroniques, pp. 30-31.

## Législations belges

Constitution coordonnée du 7 février 1831, 17 février 1994.

Code civil du 21 mars 1804, *M.B.*, 3 septembre 1807, modifié en dernier lieu par la loi du 23 mars 2019, *M.B.*, 28 mars 2019.

## Jurisprudences

C.J.U.E., 16 juillet 2009, Infopaq International A/S contre Danske Dagblades Forening, C-5/08, ECLI:EU:C:2009:465.

C.J.U.E., 8 avril 2014, Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a., C-293/12, ECLI:EU:C:2014:238.

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

C.J.U.E., 21 décembre 2016, Tele2 Sverige AB contre Post- och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a., C-203/15, ECLI:EU:C:2016:970.

C.J.U.E., 29 juillet 2019, Fashion ID GmbH & Co.KG contre Verbraucherzentrale NRW eV, C-40/17, ECLI:EU:C:2019:629.

BVerfG., EUGRZ, 1983, 588.

Cass. crim. *française*, 22 oct. 2014, n°13-82.630**.**

Tribunal de Grande instance de Créteil, 11ème chambre correctionnelle, jugement du 23 avril 2013, C13072000059.

*Ofxord v. Moss*, Divisional Court, Queens Bench (1979) 68 CR App Rep 183.

## Doctrines

AMEZ-DROZ, P. R., "Données personnelles : rente du futur?", *La tribune de Genève*, 2017. (disponible en août 2019 sur : https://archive-ouverte.unige.ch/unige:94918)

BELLANGER, P., "Les données personnelles : une question de souveraineté", *Le Débat*, 2015/1, n°183, pp. 14-25. (disponible en aout 2019 sur : https://www.cairn.info/revue-le-debat-2015-1-page-14.htm?contenu=resume)

BELLANGER P., Principes et pratiques des données personnelles en réseau, Contribution à l'étude 2014 du Conseil d'Etat : technologies numériques et libertés et droits fondamentaux, 2014.

BENABOU, V.-L.. et ROCHEFELD, J., *A qui profite le clic ? Le partage de la valeur à l'ère numérique*, Paris, Odile Jacob, 2015, 106 p.

BENSOUSSAN, A., "Pour un droit de propriété et une monétisation des données personnelles", *blog.lefigaro.fr*, février 2018.

BÉVIÈRE-BOYER, B., "Données massives en santé : ébauche d'un droit prospectif", dans *Innovation en santé publique des données personnelles aux données massives (big data)*, Paris, Librairie générale de droit et de jurisprudence, 2018, pp. 93-111.

BOURCIER, D. et DE FILLIPI, P., "Vers un droit collectif sur les données de santé", *Revue de droit sanitaire et social*, Sirey, Dalloz, 2018, 2018 (3), pp.1-14. (disponible en aout 2019 sur : https://hal.archives-ouvertes.fr/hal-01850925/)

CADOUX, L., "La protection des données personnelles en dehors de l'Europe communautaire", *Revue française d'administration publique*, janvier-mars 1999, n°89, pp. 83-103.

CATALA, P., *Les transformations du droit par l'informatique. Emergence du droit de l'informatique*, Editions des Parques, 1983, p. 264.

DE HERT, P., PAPAKONSTANTINOU, V., MALGIERI, M., BESLAY, L. and SANCHEZ, I., "The right to data portability in the GDPR: Towards user-centric interoperability of digital services", *Computer Law & Security Review*, 2018, pp. 193-203.

DE TERWANGNE, C., "Titre 5 – Droit à la vie privée: un droit sur l'information et un droit à l'information" in *Droit, normes et libertés dans le cybermonde*, Bruxelles, Éditions Larcier, 2018, pp. 555-579.

DESCHANEL, C., "L'instauration d'un droit de propriété des données personnelles : vrai danger ou fausse utilité?", *R.L.D.I.*, février 2019, n°156, pp. 35-44.

DESGENS-PASANAU, G. et FREYSSINET, E., *L'identité à l'ère numérique*, Paris, Dalloz, 2009, 170 p.

FLUECKIGER, A., "L'autodétermination en matière de donnée personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété?", *Pratique juridique actuelle*, 2013, vol. 22, n°6, pp. 837-864. (disponible en août 2019 sur : https://archive-ouverte.unige.ch/unige:30735)

FLYNN, C., "Shortcomings of the EU proposal for free flow of data", *InterMEDIA*, 2018, Vol 45, Issue 4, pp. 30-35.

GATES, C., MATTHEWS, P., "Data is the New Currency", *NSPW '14 proceeding of the 2014 New Security Pardigms Workshop*, Victoria British Columbia Canada, 2014, pp. 105-116.

GUTWIRTH, S., GONZALEZ FUSTER, G., "Titre 5 - L'éternel retour de la propriété des données de l'insistance d'un mot d'ordre" in *Droit, normes et libertés dans le cybermonde*, Bruxelles, Éditions Larcier, 2018, pp. 117-140.

HAYAT, O. et HUIN, L., "Un régime juridique européen sur les données non personnelles", *Expertise*, janvier 2019, pp. 32-37.

JANECEK, V., "Ownership of personnal data in the internet of Things", *Computer Law & Security Review*, 2018, n°0, pp. 1-14.

KNOCKAERT, M. et TOMBAL, T., "Quels droits sur les données?", Conférence Actualités en droit du numérique, 42e session, Mons, mai 2019.

LANDREAU, I., PELIKS, G., BINCTIN, N. et PEZ-PÉRARD, V. sous la direction de LÉGER, L., "Créer une patrimonialité des données à droit constant.", dans le rapport "Mes datas sont à moi." du collectif Génération Libre, janvier 2018, pp. 46-100. (disponible sur : https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf)

LAROCHE, M., "Vers un renouvellement de la propriété? Les fonctions du droit de propriété.", *Propriété(s) et données*, décembre 2016, Paris, France, 9 p. (disponible en aout 2019 sur : https://hal.archives-ouvertes.fr/hal-02090602/)

LEMPÉRIÈRE, M., "Les transferts de données vers le Royaume-Uni après le Brexit", *Expertise*, avril 2019, pp. 138-141.

LEROY, F., *Réseaux sociaux & Cie : le commerce des données personnelles*, Arles, Actes Sud, 2013, 263 p.

MALGIERI, G. and CUSTERS, B., "Pricing privacy: the right to know the value of your personal data", *Computer Law & Security Review*, 2018, n°34, pp.289-303.

MALGIERI, G. et DE HERT, P, "Making the most of new laws: reconciling big data innovation and personal data protection within and beyond the GDPR" in E Degrave, C de Terwangne, S Dusollier & R Queck (eds), *Law, Norms and Freedoms in Cyberspace - Droit, Norme et Libertés dans le Cybermonde: Liber Amicorum Yves Poullet.* 2018, Larcier, Bruxelles, pp. 525-554.

MATTATIA, F. et YAÏCHE, M., "Etre propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété? (Partie I)", *R.L.D.I.*, mai 2015, n°115, pp. 63-65.

MATTATIA, F. et YAÏCHE, M., "Etre propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété? (Partie II)", *R.L.D.I.*, juin 2015, n°116, pp. 41-44.

MICHOT-CASBAS, M. et HERVÉ C., "Introduction - Les données massives en santé : enjeux éthiques des Big Dta dans la réalité des soins", dans *Innovation en santé publique des données personnelles aux données massives (big data),* Paris, Librairie générale de droit et de jurisprudence, 2018, pp. 1-11.

MOURBY, M., MACKEY, E., ELLIOT, M., GOWANS, H., WALLACE, S., BELL, J., SMITH, H., AIDINLIS, S. and KAYE J., "Are «pseudonymised» data always personal data? Implications of the GDPR for administrative data research in the UK", *Computer Law & Security Review*, 2018, n°34, pp. 222-233.

MOURON, P., "Pour ou contre la patrimonialité des données personnelles", *Revue Européenne des Médias et du Numérique,* n°46-47, printemps-été 2018, pp.90-96.

MÜLLER, J.K.M., "Dateneigentum in der vierten industriellen Revolution?", *Datenschutz und Datensicherheit*, 2019/3, pp. 159-166.

PADOVA, Y., "Entre patrimonialité et injonction au partage : la donnée écartelée? (Partie I)", *R.L.D.I.*, janvier 2019, n°155, pp. 47-56.

PADOVA, Y., "Entre patrimonialité et injonction au partage : la donnée écartelée? (Partie II)", *R.L.D.I.*, février 2019, n°156, pp. 45-51.

POULLET, Y., "Le fondement du droit à la protection des données nominatives : « Propriétés ou Libertés »", Nouvelles technologies et propriétés, novembre 1989, pp. 175-205.

POULLET, Y., "Les concepts fondamentaux de la protection des données et les nouvelles technologies de l'information", Dr. Infrom., 1987/4, pp. 222-227.

PRINS, J.E.J., "The propertization of personal data and identities", *Electronic Journal of Comparative Law*, vol. 8.3, october 2004, 7 p. (available at https://www.researchgate.net/publication/247957565_The_Propertization_of_Personal_Data_and_Identities)

PUCHERAL, P., RALLET, A., ROCHELANDET, F. et ZOLYNSKI, C., "La privacy by design : une fausse bonne solution aux problèmes de protection des données personnelles soulevés par l'open data et les objets connectés ?", Victoire éditions, 2016/1, n°51, pp. 89-99. (disponible en aout 2019 sur : https://hal.archives-ouvertes.fr/hal-01427983)

PURTOVA, N., *Property right in personal data : a European perspective*, Alphen aan den Rijn, Kluwer, 2012 308 p.

PURTOVA, N., "Property right in personal data: Learning from the American discourse", *Computer Law & Security Review*, 2009, n°25, pp. 507-521.

PURTOVA, N., "The illusion of personal data as no one's property", *Law Innovation and Technology*, 2015, pp 83-111. (available at : https://www.tandfonline.com/doi/abs/10.1080/17579961.2015.1052646)

RALLET, A. et ROCHELANDET, F., "La régulation des données personnelles face au web relationnel : une voie sans issue ?", *Réseaux*, 2011/3, n°167, pp. 17-47. (disponible en août 2019 sur : https://www.cairn.info/revue-reseaux-2011-3-page-17.htm)

RALLET, A., ROCHELANDET, F. Et ZOLYNSKI, C., "De la privacy by design à la privacy by using", *Réseaux*, 2015/1 (n°189), pp. 15-46. (disponible en août 2019 sur https://www.cairn.info/revue-reseaux-2015-1-page-15.htm?contenu=article)

RALLET, A., "Valoriser ses données personnelles ? 3 scénarios", *Document de travail*, Université de Paris Saclay, octobre 2018, 21 p. (disponible en août 2019 sur https://hal.archives-ouvertes.fr/hal-01909650/document)

REARDON, J., FEAL, A., WIJESEKERA, P., ELAZARI BAR ON, A., VALLINA-RODRIGUEZ, N. and EGELMAN, S., "50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System", submitted to FTC PrivacyCon2019, 18 p. (available at : https://www.ftc.gov/system/files/documents/public_events/1415032/privacycon2019_serge_egelman.pdf)

ROBERT, R., "Peut-on payer avec ses données personnelles : La proposition de directive « contenu numérique » introduit le ver dans le fruit", *J.T.D.E.*, 2017, n° 9, pp. 356-358.

ROCHELANDET, F., *Economie des données personnelles et de la vie privée*, Paris, La Découverte, 2010, 125 p.

ROSIER, K., "Titre 12 - La notion de « donnée à caractère personnel » a-t-elle encore un sens dans la protection des données de communications électroniques" in *Droit, normes et libertés dans le cybermonde*, Bruxelles, Éditions Larcier, 2018, pp. 699-714.

RUBINSTEIN, I., "Big Data: The End of Privacy or a New Beginning?", *New York University School of Law Public Law & Legal Theory research paper series*, working paper n°12-56, october 2012, 14 p. (available at : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2157659)

SAINT-AUBIN, T., "Les nouveaux enjeux juridiques des données (big data, web sémantique et linked data)", *R.L.D.I.*, mars 2014, n°102, pp. 94-101.

STRAKER, C., "From data property to data rights: Legal thoughts on basic principles of the European digital economy in the age of Big Data", *R.D.T.I.*, 2018, n°70, pp. 63-74.

STREEL, A., "Titre 4 - Les données, l'innovation et le droit des concentrations" in *Droit, normes et libertés dans le cybermonde*, Bruxelles, Éditions Larcier, 2018, p. 109-116.

STROWEL, A.,"Titre 10 - Les données des ressources en quête de propriété" in *Droit, normes et libertés dans le cybermonde*, Bruxelles, Éditions Larcier, 2018, pp. 251-268.

TUBERT, S. et ZIEGLER, L., "Propriété intellectuelle et données personnelles à l'épreuve du deep learning", *Expertises*, Janvier 2019, n°442, pp. 16-25.

ZECH, H., "Data as a Tradeable Commodity – Implications for Contract Law", Josef Drexl (ed.), Proceedings of the 18th EIPIN Congress: The New Data Economy between Data Ownership, Privacy and Safeguarding Competition, *Edward Elgar Publishing*, Forthcoming, 2017, 15 p. (Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063153)

## Articles et sites consultés en ligne

AFP, "Facebook étudie l'impact des réseaux sociaux sur les élections", publié le 30 avril 2019 sur *latribune.fr* (disponible depuis ce lien : https://www.latribune.fr/technos-medias/facebook-etudie-l-impact-des-reseaux-sociaux-sur-les-elections-815752.html).

BATHELOT, B., "Définition : Effet Streisand", 18 décembre 2018 sur *définitions-marketing.com* (disponible depuis ce lien : https://www.definitions-marketing.com/definition/effet-streisand/).

BELGA, "Facebook : le régulateur américain en faveur d'une amende de 5 milliards de dollars", 12 juillet 2019 sur lesoir.be (disponible depuis ce lien : https://www.lesoir.be/236331/article/2019-07-12/facebook-le-regulateur-americain-en-faveur-dune-amende-de-5-milliards-de-dollars?).

CHERIF, A., "Être propriétaire de ses données personnelles, une dangereuse illusion", 23 mars 2018 sur *latribune.fr* (disponible en aout 2019 sur https://www.latribune.fr/technos-medias/internet/etre-proprietaire-de-ses-donnees-personnelles-une-dangereuse-illusion-773398.html)

CIMINO, V., "Google détecte le cancer du sein métastatique avec une précision de 99%", 15 octobre 2018 sur *siecledigital.fr* (disponible depuis ce lien : https://siecledigital.fr/2018/10/15/une-ia-by-google-detecte-le-cancer-avec-une-precision-de-99/).

CONESA, E., "La France adopte la taxe GAFA malgré les menaces de Trump", 11 juillet 2019 sur *lesechos.fr* (disponible depuis ce lien : https://www.lesechos.fr/monde/etats-unis/la-france-adopte-la-taxe-gafa-malgre-les-menaces-de-trump-1037413).

DUGUA, P., "Donald Trump attaque la France sur la taxe Gafa", 11 juillet 2019 sur *lefigaro.fr* (disponible depuis ce lien : http://www.lefigaro.fr/conjoncture/donald-trump-ordonne-une-enquete-sur-la-taxe-gafa-prelude-a-des-sanctions-20190711).

E. STEEL, E., LOCKE, C., CADMAN, E., et FREESE, B., "How much is your personal data worth ?", publié le 12 juin 2013 sur *financialtime.com* (disponible depuis ce lien : https://ig.ft.com/how-much-is-your-personal-data-worth/).

FALJAOUI, A., "Comment WhatsApp et Facebook ont influencé l'élection au Brésil", publié le 5 novembre 2018 sur *rtbf.be* (disponible depuis ce lien : https://www.rtbf.be/classic21/article/detail_comment-whatsapp-et-facebook-ont-influence-l-election-au-bresil?id=10064682).

GUERGUINOV, O. et WERY, E., "La donnée non-personnelle (anonyme) existe-elle ?", 1 aout 2019 sur *droit-technologie.org* (disponible depuis ce lien : https://www.droit-technologie.org/actualites/la-donnee-non-personnelle-anonyme-existe-elle/?fbclid=IwAR0J9JlhYy7-o1-Lk7ZXk7YBfPECfnmajO21WI9XGERvSeHypYNSm7jJR4I).

HARRISON, S., "Can you make money selling your data", 21 septembre 2018 sur *bbc.com* (disponible depuis ce lien : http://www.bbc.com/capital/story/20180921-can-you-make-money-selling-your-data).

HERPIN, T., "[Infographie] Les GAFAM et la répartition de leur chiffre d'affaire en 2017", 25 avril 2018 sur *ecommerce-nation.fr* (disponible depuis ce lien : https://www.ecommerce-nation.fr/gafam-repartition-chiffre-daffaires-2017/).

LAUSSON, J., "La CNIL inflige à Google une amende record de 50 millions d'euros pour violation du RGPD", 21 janvier 2019 sur *numerama.fr* (disponible depuis ce lien : https://www.numerama.com/politique/457010-la-cnil-inflige-a-google-une-amende-record-de-50-millions-deuros-pour-violation-du-rgpd.html).

LE SOIR, "« La stupidité de Macron » : Trump menace le vin français en réponse à la taxe GAFA", 27 juillet 2019 sur *lesoir.be* (disponible depuis ce lien : https://www.lesoir.be/238819/article/2019-07-27/la-stupidite-de-macron-trump-menace-le-vin-francais-en-reponse-la-taxe-gafa).

LECOMTE, E., "L'IA de Microsoft est-elle réellement devenue raciste au contact des internautes ?", 25 mars 2016 sur *sciencesetavenir.fr* (disponible depuis ce lien : https://www.sciencesetavenir.fr/high-tech/intelligence-artificielle/l-ia-de-microsoft-est-elle-reellement-devenue-raciste-au-contact-des-internautes_31260).

MATYSZCZYK, C., "Google bought my friend's face for $5", 21 juillet 2019 sur zdnet.com (disponible depuis ce lien : https://www.zdnet.com/article/google-bought-my-friends-face-for-5/).

MASSARD, J., "Trump riposte à la « taxe GAFA » française", 11 juillet 2019 sur *euronews.com* (disponible depuis ce lien : https://fr.euronews.com/2019/07/11/trump-riposte-a-la-taxe-gafa-francaise).

RÉDACTION DE MÉDIAPART , "Combien valent vos données personnelles ?", publié le 15 juillet 2013 sur *médiapart.fr* (disponible depuis ce lien : https://www.mediapart.fr/journal/economie/150713/combien-valent-vos-donnees-personnelles).

RT FRANCE, "Interdit d'interdire : A qui profite la collecte de nos données personnelles?", Diffusé en direct le 22 oct. 2018 (accessible sur *Youtube* en juillet 2019 depuis ce lien : https://www.youtube.com/watch?v=BWINrcIaXFA).

SALOVIC, B., LÉONARD, T., WERY, E., "Bouton « j'aime » de Facebook : voici le verdict final de la CJUE", 29 juillet 2019 sur droit-technologie.fr (disponible depuis ce lien : https://www.droit-technologie.org/actualites/bouton-jaime-de-facebook-voici-le-verdict-final-de-la-cjue/).

SCIENCEETONNANTE , "Le deep learning - Science étonnante #27", mis en ligne le 8 avril 2016 (disponible sur *Youtube* en aout 2019 depuis ce lien : https://www.youtube.com/watch?v=trWrEWfhTVg).

SCIENCES ET AVENIR et AFP, "Une intelligence artificielle capable de reconnaitre le mélanome avec 95% d'efficacité", 29 mai 2018 sur *sciencesetavenir.fr* (disponible depuis ce lien : https://www.sciencesetavenir.fr/sante/dermato/cancer-de-la-peau-une-intelligence-artificielle-meilleure-dans-le-depistage-que-les-dermatologues_124423).

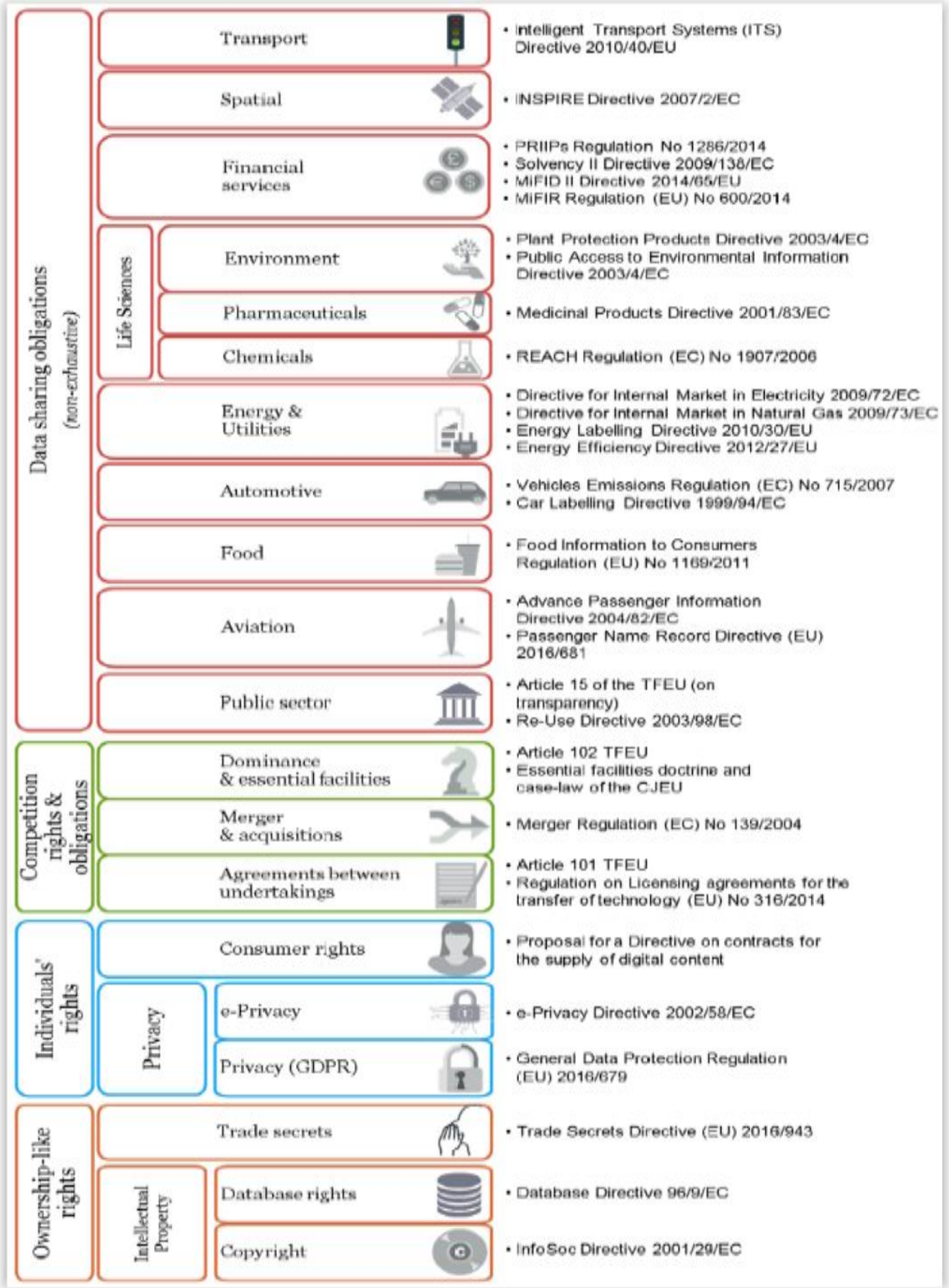
SERMONDADAZ, S., "Numérique et écologie : les data centers, des gouffres énergétiques ?", 9 mars 2018 sur *sciencesetavenir.fr* (disponible depuis ce lien : https://www.sciencesetavenir.fr/high-tech/informatique/numerique-et-ecologie-les-data-centers-des-gouffres-energetiques_121838).

SIGNORET, P., "Amazon a du désactiver une IA qui discriminait les candidatures de femmes à l'embauche", 10 octobre 2018 sur *numerama.com* (disponible depuis ce lien : https://www.numerama.com/tech/426774-amazon-a-du-desactiver-une-ia-qui-discriminait-les-candidatures-de-femmes-a-lembauche.html).

TUAL, M., "A peine lancée, une intelligence artificielle de Microsoft dérape sur twitter", 24 mars 2016 sur *lemonde.fr* (disponible depuis ce lien : https://www.lemonde.fr/pixels/article/2016/03/24/a-peine-lancee-une-intelligence-artificielle-de-microsoft-derape-sur-twitter_4889661_4408996.html).

VERSET, J.-C., "Internet bientôt premier consommateur mondial d'électricité", 10 avril 2018 sur *rtbf.be* (disponible depuis ce lien : https://www.rtbf.be/info/economie/detail_internet-bientot-premier-consommateur-mondial-d-electricite?id=9889099).

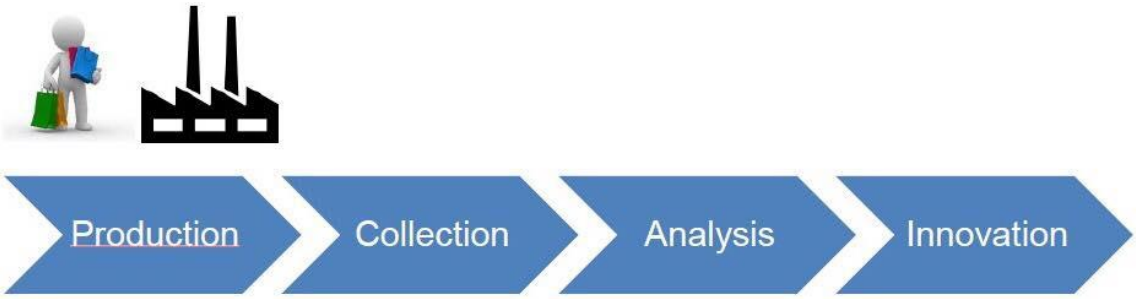
**Annexe 1 :** (source : KNOCKAERT, M. et TOMBAL, T., "Quels droits sur les données?", Conférence Actualités en droit du numérique, 42e session, Mons, mai 2019.)



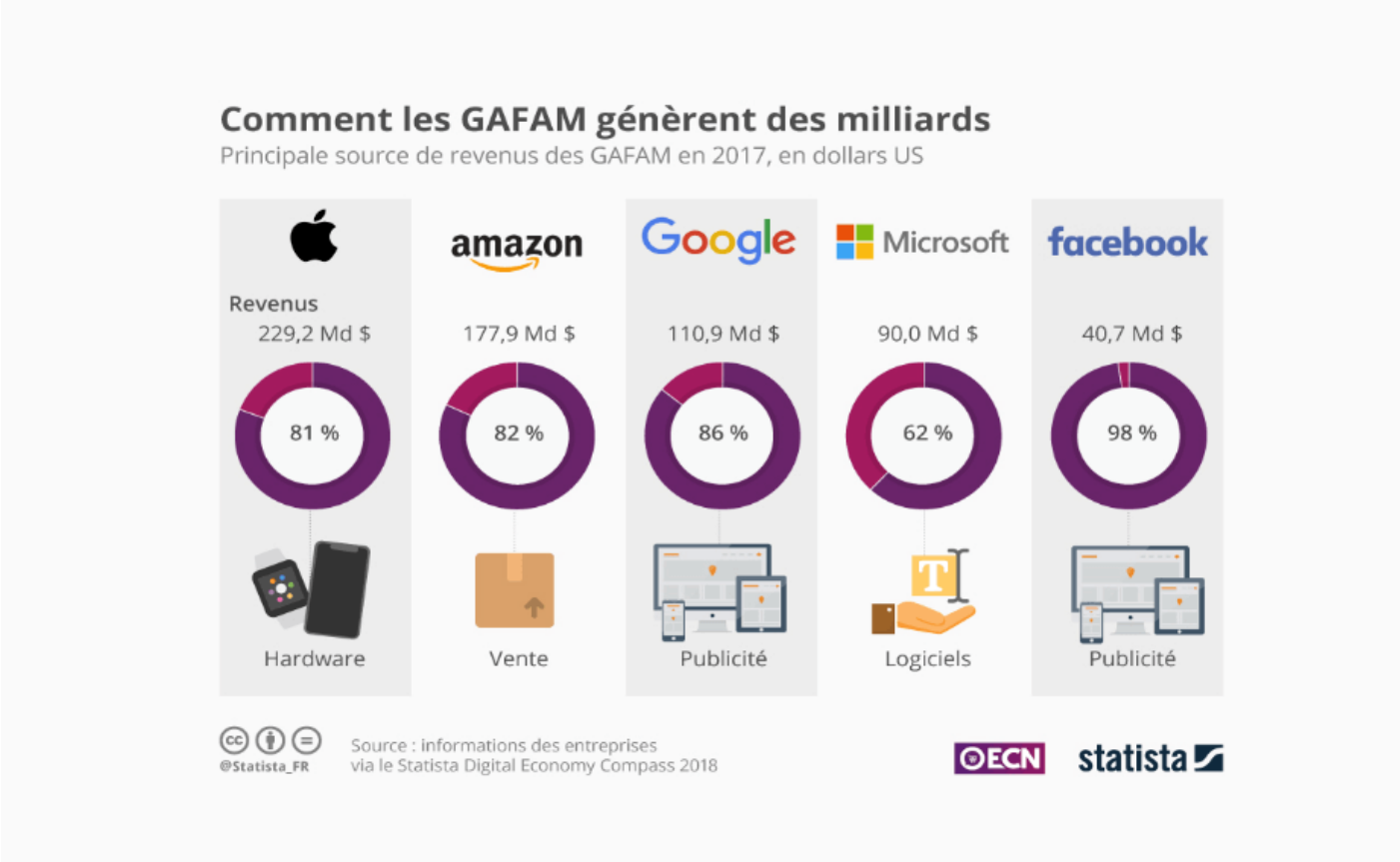
**Annexe 2 :** (source : ZECH, H., "Data as a Tradeable Commodity – Implications for Contract Law", Josef Drexl (ed.), Proceedings of the 18th EIPIN Congress: The New Data Economy between Data Ownership, Privacy and Safeguarding Competition, *Edward Elgar Publishing*, Forthcoming, 2017, 15 p. (Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063153))

2.1 Data Value Chains

The simplest form of schematising the data economy would look like this:[4]




**Annexe 3 :** (source : T. HERPIN, "[Infographie] Les GAFAM et la répartition de leur chiffre d'affaire en 2017", 25 avril 2018 sur *ecommerce-nation.fr* (disponible depuis ce lien : https://www.ecommerce-nation.fr/gafam-repartition-chiffre-daffaires-2017/).)



# *Table des matières*

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