UCLouvain

Faculté de droit et de criminologie

Quantified self et RGPD : Quel contrôle sur nos données personnelles ?

Mémoire en droit des nouvelles technologies

Auteur : DELATTE François

Promoteur : LAZARO Christophe

Année académique 2018-2019

Master en droit à finalité droit de l'entreprise

Plagiat et erreur méthodologique grave

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

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

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

* À ce sujet, voyez notamment **http://www.uclouvain.be/plagiat**

Remerciements

Je souhaiterais remercier l'ensemble des personnes qui ont été impliquées de près ou de loin dans la rédaction de ce mémoire. Mes recherches n'auraient pu aboutir sans l'aide précieuse de l'ensemble d'entre elles.

Je tiens en premier lieu à remercier le Professeur Christophe Lazaro d'avoir assumé le rôle de promoteur. De par nos multiples réunions constructives, il m'a apporté soutien, idées et remises en question. Je souhaite également le remercier d'avoir pris le temps de lire plusieurs fois les versions intermédiaires de mon travail pour y apporter des commentaires aussi nombreux que constructifs.

Je souhaite également remercier Monsieur Laurent Baijot, CEO de l'application belge de quantified self Formyfit, de m'avoir accordé de son temps. Durant notre interview et grâce à son expérience de terrain, il a su confirmer mes recherches théoriques ainsi que donner une dimension pratique à mon travail.

En outre, mes plus chaleureux remerciements vont à mes re-lecteurs, Marine et mes parents, Anne et Benoît, qui ont su, par leurs pertinentes remarques, me remettre sur le bon chemin tant sur le fond que sur la forme.

Enfin, je souhaiterais adresser mes remerciements à ma famille et à mes amis, François et Logan, pour les nombreux moments d'échange autour de ce travail et pour le soutien mutuel durant nos recherches et rédactions.

« Nous vivons dans une société dépendant de manière exquise de la science et de la technologie, dans laquelle presque personne ne sait quelque chose sur la science et la technologie. »

Carl Sagan

Table des matières

Introduction générale 1

Chapitre 1. Le quantified self 3

Section 1. Définitions et contours 3

§1 La chaine du quantified self 4

§2 Des pratiques au mouvement 5

§3 Le quantified self en quelques chiffres 7

A. Le marché 7

B. Modèle économique et prix moyen 9

i. Les traqueurs 9

ii. Les applications 10

iii. L'expansion vers le business to business 12

Section 2. Le quantified self en pratique 13

Sous-Section 1. Les outils du quantified self 13

§1 Les applications automatisées 13

A. Le sport 13

B. Le sommeil 17

§2 Les applications manuelles 18

A. L'alimentation 18

B. L'humeur 19

§3 Les traqueurs 21

Sous-Section 2. Les utilisations dérivées du quantified self et leurs risques 24

§1 La justice 24

§2 Les assurances 25

Section 3. Analyse approfondie du mouvement 27

§1 Mesure et quantification 27

§2 La communauté 28

Chapitre 2. Les données personnelles et le quantified self 32

Introduction 32

Section 1. Le cadre législatif 33

Section 2. Les notions fondamentales du règlement 35

Sous-Section 1. Données à caractère personnel 35

§1 Les informations 36

§2 Les personnes concernées *36*
A. Personne physique 37
B. Concernée 37
C. Identifiée ou identifiable 38
§3 Les données sensibles *39*
Sous-Section 2. Traitement ***41***
§1 Notion *41*
§2 Principe de loyauté et de transparence *41*
§3 Finalité déterminée et explicite *42*
§4 Principe de licéité du traitement *43*
A. Le consentement 43
i. Notion 44
• Définition 44
• Par une déclaration ou un acte positif clair 44
ii. Qualités du consentement 45
• Libre 45
• Spécifique 46
• Éclairé 47
• Univoque 47
iii. Retrait du consentement 48
B. Le contrat 49
§5 Traitement de données sensibles *50*
Sous-Section 3. Responsable du traitement et sous-traitant ***51***
§1 Le responsable du traitement *51*
§2 Le sous-traitant *53*
§3 Principe d'« accountability » *53*
Sous-Section 4. Champ d'application territorial ***54***
§1 Établissement d'un responsable du traitement ou sous-traitant au sein de l'Union Européenne *54*
§2 Pas d'établissement au sein de l'Union Européenne *55*
A. Offre de biens ou de services au sein de l'Union Européenne 55
B. Le suivi d'un comportement 56
Sous-Section 5. Conclusion intermédiaire ***57***
Chapitre 3. Contrôler ses données : utopie législative ou réalité ? **58**
Section 1. Définition du contrôle **58**

Section 2. Analyse pratique de la portée du contrôle envisageable par la personne concernée 59

§1 La notion de consentement 59

A. Le consentement en général 59

B. La notion de consentement explicite au sein d'outils de quantified self 62

C. Le droit au retrait et à l'effacement 62

D. Conclusion sur le consentement 63

§2 Le contrat 63

§3 Les pratiques au sein des entreprises actives dans le quantified self 63

§4 Conclusion intermédiaire 64

Section 3. Initiatives tierces au règlement afin de rendre le contrôle de leurs données aux personnes concernées 65

§1 Repenser les politiques de vie privée 65

§2 Le self data 67

A. Notion 67

B. Le Blue Button 68

Conclusion 70

Bibliographie 72

Annexe : Interview Laurent Baijot : CEO ForMyFit 82

Introduction générale

Quantified self, données personnelles sensibles, traqueurs, Apple Watch, Runtastic,… Voici des mots qui sont nés récemment et dont nous ne saisissons pas toujours la portée. Ils sont souvent associés à une technologie obscure, à des multinationales ou encore au *BigBrother* tel que décrit par George Orwell dans son ouvrage 1984.

En quelques mots, le *quantified self* désigne un mouvement de personnes souhaitant objectiver leurs activités sportives ou quotidiennes dans le but d'obtenir des données afin de pouvoir s'améliorer. Il existe des dispositifs permettant de quantifier la course à pied, le sommeil, l'alimentation ou encore l'humeur.

Auparavant, ces données ne pouvaient être analysées que via la tenue d'un carnet papier relatant les données que les utilisateurs souhaitaient analyser, les données recueillies étaient donc limitées. Désormais, il est possible via des applications ou traqueurs, de récolter une infinité de données sur nous même et notre environnement. La conséquence est que la détention des données a changé de camp. Elle est passée de l'utilisateur à l'entreprise qui a commercialise l'outil de *quantified self* utilisé.

Cette nouvelle entrée sur le marché est perçue de façon ambivalente. Entre ceux qui voient en ces objets une technologie révolutionnaire et ceux qui les perçoivent comme de nouvelles façons de subtiliser nos données personnelles afin de nous épier encore plus. Il est nécessaire d'y voir plus clair. Ce qui est d'autant plus frappant, c'est que nombre de citoyens se fient à cette technologie pour objectiver leurs vies mais très peuvent savent réellement comment cela fonctionne et quelles implications allant au delà de cette quantification cela peut avoir pour leurs vies.

La récente entrée en vigueur du règlement général sur la protection des données à caractère personnel nous est parue comme une véritable opportunité de confronter deux visions du *quantified self*. L'une ayant trait à la technologie, à ce qu'elle est capable de nous apporter et l'autre concernant les traitements de données à caractère personnel sous-jacents à ces activités.

Quels sont ces appareils qui font partie du *quantified self* ? Quelles sont les données collectées par ces appareils ? Sommes-nous capables de donner notre consentement au traitement de ces données ? Qu'en dit la loi ? Les concepts mis en place sont-ils suffisants pour protéger les utilisateurs, et le cas échéant, que peut on faire pour y pallier ? Nous tenterons d'y répondre au sein de cette contribution.

Dans une première partie, nous nous essaierons à la définition ainsi qu'à l'analyse du outils du *quantified self*. Ensuite, nous nous attarderons sur quelques implications sociologiques concernant ce mouvement.

Dans une seconde partie, nous confronterons cette vision du *quantified self* à une analyse du règlement général sur la protection des données. Nous y étudierons les notions fondamentales du règlement et nous approfondirons les notions importantes concernant le traitement de données par les applications et traqueurs analysés précédemment. Les questions de légitimation du traitement via le consentement ou le contrat y seront centrales.

Dans une troisième et ultime partie, nous émettrons nos critiques par rapport aux questions précédemment analysées. La question traitée étant de savoir si les ressources mises en place par le règlement face aux outils de *quantified self* sont suffisantes pour permettre un contrôle des données par l'utilisateur. Nous apporterons également certaines pistes de solutions externes au règlement.

En ce qui concerne notre méthode, nous souhaitions mettre en exergue certains choix opérés au sein de ce mémoire. En tant qu'utilisateur d'outils de *quantified self*, notamment de l'application Strava et d'une montre Apple Watch, cette utilisation nous a permis d'obtenir une meilleur connaissance du sujet en se mettant directement dans la peau de l'utilisateur tel que détaillé au sein de la présente contribution. C'est cette même utilisation d'outils qui a donné une dimension résolument pratique aux analyses réalisées-ci dessous. Il en découle naturellement que certains exemples de ce mémoire sont purement personnels et issus de notre pratique.

Nous avons mis un point d'honneur à étayer notre propos théorique par des incises pratiques. Cela passe notamment par cette immersion décrite ci dessus mais également par une rencontre avec un professionnel du secteur. Dans cette optique, nous avons rencontré Monsieur Laurent Baijot, co-fondateur de l'application *Formyfit*. Durant cette entrevue, retranscrite en annexe, nous avons pu recevoir de précieuses considérations pratiques afin d'étoffer notre propos.

Chapitre 1. Le quantified self

Notre analyse débute par une première approche de la matière du *quantified self* qui permettra de se représenter ce qui se cache derrière ce concept qui, aux premiers abords, peut sembler abstrait. Après un premier exercice de définition et de présentation du mouvement, nous poursuivrons vers la description des outils employés par les utilisateurs ainsi que des implications sociologiques propres à ce mouvement.

Section 1. Définitions et contours

Le *quantified self* est perçu de façon uniforme et, malgré le fait qu'il n'en existe pas de définition officielle, ses contours ne donnent pas lieu à débat. Dans le cadre de ce propos volontairement limité, nous ne traiterons cependant pas du quantified self appliqué aux usages médicaux.

Voici plusieurs définitions qui circonscrivent le sujet :

« Ce mouvement [le *quantified self*] concerne l'utilisation d'outils numériques portables ainsi que des technologies intégrant des senseurs qui permettent à leurs utilisateurs d'enregistrer des données à propos de leurs activités quotidiennes et d'obtenir un retour sous forme de graphes et d'illustrations. »[1]

« Le *quantified self* est une zone émergente de la technologie qui permet aux consommateurs d'utiliser une variété d'outils pour collecter des données à propos de leurs comportements et de leurs habitudes de tous les jours. »[2]

« [Le *quantified self*] est un phénomène large qui consiste en une variété d'aspects : l'utilisation d'outils numériques, le stockage et l'interprétation de données qui résultent des mesures, l'analyse de ces données et finalement la connaissance de soi. »[3]

---

[1] B. AJANA, « Digital health and the biopolitics of the quantified self », *Digital Health*, Londres, 2017, Vol. 3., p. 2, disponible en ligne à l'adresse : https://www.researchgate.net/publication/312090206_Digital_Health_and_the_Biopolitics_of_the_Quantified_Self, consulté le 19 février 2019, traduction libre.

[2] Rocket fuel, *"quantified self " digital tools a cpg marketing opportunity*, 2014, p. 1, traduction libre.

[3] E. BIRKAVS, M. KOEDIJK, X. MING et B. WOLBERS, *The Quantified Self - Self-knowledge Through Numbers?*, Twente, Technolab, 2017, p.2, disponible en ligne : http://www.ideefiks.utwente.nl/wp_base/wp-content/uploads/2016/01/Final-Project-Quantified-Self-6_22_2016.pdf, consulté le 16 février 2019, traduction libre.

En résumé, le *quantified self* est un mouvement au sein duquel, des pratiquants récoltent des données au sujet de leurs activités quotidiennes (sport, sommeil, alimentation,…) dans le but d'objectiver ce qui se passe dans leur vie et de pouvoir améliorer celle-ci.[4]

§1 La chaine du quantified self

Ce mouvement est également souvent représenté par la chaine du *quantified self*. Ce terme utilisé pour faire référence à l'usage d'outils technologiques tels que les traqueurs d'activités donne lieu à des pratiques qui regroupent une chaine d'actions.[5] Celles-ci sont : « *Self→ Measurement→ Data→ Information→ Knowledge→ Improvement* ».[6] Cette chaine résume le cheminement effectué par les adeptes du mouvement car elle suit toutes les étapes par lesquelles il faut passer afin d'améliorer ce que l'on mesure.

Prenons un exemple afin d'expliciter ce cheminement : un sportif en herbe rêve de réaliser un marathon. Il court toutes les semaines mais ne progresse pas. Il décide alors d'acheter un bracelet connecté afin de connaitre ses performances.

Le processus commence par la personne elle-même qui est le sujet mesuré, c'est à dire le sportif. À partir de là, il va porter le bracelet sur lui (*self*) pendant ses séances afin de savoir comment il court (*measurement*). De ces séances, il va retirer des données qui auront été collectées (*data*), ces données (distance, durée, rythme cardiaque,…) vont pouvoir l'informer sur ce qu'il a réalisé (*information*). Il va par exemple se rendre compte, qu'il ne court qu'un seul kilomètre à chaque séance (*knowledge*), ce qui va lui permettre de savoir qu'il doit courir des distances plus longues afin de réaliser un marathon (*improvement*).

La connaissance n'est donc pas la seule chose qui compose ces pratiques, il existe de nombreuses étapes préalables à cette connaissance. Nous sommes donc en présence d'un processus complexe d'établissement d'une vérité présumée scientifique. En outre, cette connaissance n'est pas le point

---

[4] K. KELLY, dans TAKASHI D., Quantifiying our lives will be a top trend in 2012, disponible à l'adresse : « https://venturebeat.com/2012/01/21/quantifying-our-lives-will-be-a-top-trend-of-2012/ », consulté le 13 mars 2019.

[5] J. LAURENT, « Healthscapes of self-quantification : Quantifying, knowing and improving one's self: transforming health », *eä Journal*, 2015, Vol. 7, n° 1, p. 111.

[6] E. BIRKAVS, M. KOEDIJK, X. MING et B. WOLBERS, *The Quantified Self - Self-knowledge Through Numbers?*, *Op, Cit.*, p.2.

final de ce processus, c'est son utilisation qui est primordiale.[7] En effet, réaliser un tel parcours pour obtenir ces informations sans tirer de conséquences le place au même stade qu'avant ce processus.

§2 Des pratiques au mouvement

Malgré le fait que ces pratiques soient souvent perçues comme relativement récentes, il existe des traces de pratiques similaires depuis le 19ème siècle. C'est à cette époque que se sont développées les statistiques et que l'on a commencé à comprendre le monde qui nous entoure par les chiffres, perçus comme objectifs et neutres.[8]

Le terme « *Quantified Self* » a été utilisé pour la première fois par Gary WOLF et Kevin KELLY en 2007.[9] L'élaboration de ce terme a permis de regrouper toute une série de pratiques, qui sont des actions désordonnées et pratiquées isolément par des individus en un mouvement.[10] Un mouvement, est, quant à lui, formé des pratiques coagulées et convergentes.[11]

Les pratiques qui forment ce mouvement concernent la récolte de données variées à propos du corps afin de pouvoir comprendre ce qu'il s'y passe et de pouvoir l'améliorer. C'est donc une nouvelle opportunité pour chacun d'optimiser son quotidien ou ses résultats.[12]

Ce qui a fait passer ces pratiques au statut de mouvement est notamment l'organisation de rencontres réunissant les adeptes du *quantified self*.[13] Ces réunions s'articulent autour de trois questions phares : « *What did you do? ; How did you do it? ; What did you learn?* ».[14]

---

[7] J. LAURENT, « Healthscapes of self-quantification : Quantifying, knowing and improving one's self: transforming health », *op. cit.*, pp. 115 et 116.

[8] M. KOEDIJK, « *A brief historical introduction to the quantified self* », The Quantified Self - Self-knowledge Through Numbers?, Twente, Technolab, 2017, p. 8, disponible en ligne : http://www.ideefiks.utwente.nl/wp_base/wp-content/uploads/2016/01/Final-Project-Quantified-Self-6_22_2016.pdf, consulté le 16 février 2019.

[9] C. GICQUEL, P. GUYOT, Quantified self, les apprentis sorciers du « moi connecté », Paris, FYP éditions, 2015, p.58; Voy. aussi, http://quantifiedself.com/2011/03/what-is-the-quantified-self/, consulté le 12 février 2019; Voy. aussi E. BIRKAVS, M. KOEDIJK, X. MING et B. WOLBERS, *op. cit.,* p. 3.

[10] J. LAURENT, « Healthscapes of self-quantification : Quantifying, knowing and improving one's self: transforming health », *op. cit.*, p. 111.

[11] J. LAURENT, *Ibid.,* p. 111.

[12] E. BIRKAVS, M. KOEDIJK, X. MING et B. WOLBERS, *op. cit.,* p. 2.

[13] B. ARRUABARRENA, *Le Soi augmenté : les pratiques numériques de quantification de soi comme dispositif de médiation pour l'action*, Sciences de l'information et de la communication, Conservatoire national des arts et metiers - CNAM, 2016, p. 16.

[14] G. WOLF, *Our three prime questions*, Quantified self website, 2011, disponible sur : http://quantifiedself.com/2011/09/our-three-prime-questions/, consulté le 17 février 2019 ; Voy. aussi, N. DOW SCHÜLL, Self in the loop : « Bits patterns, and pathways in the quantified self », *in The Networked Self*, 2018, New York, Vol 5: Human Augmentics, Artificial Intelligence, Sentience, Ed. Zizi Papacharisi p. 27.

Ces réunions informelles ont été un moyen de populariser les pratiques et le mouvement en général. Autour des celles-ci, se sont développés un site et un forum qui ont aussi permis de donner une dimension plus globale au mouvement.[15]

L'émergence du mouvement est également due à une nouvelle stratégie plus ambitieuse des entreprises face au business du *quantified self*. Celles-ci, surfant sur la vague, se sont mises à produire de plus en plus d'applications et de capteurs afin de toucher le plus de consommateurs.[16]

Certains considèrent que le *quantified self* n'est pas né uniquement de l'évolution de la technologie mais également d'un changement de mentalité au sein de la population. Au travers de ces équipement, chacun est désormais capable de prendre en main sa santé.

Selon LUPTON,[17] le *quantified self* est en partie né d'une volonté des individus de se ré-approprier leur santé. Celle-ci parle d'une responsabilisation croissante des citoyens dans leur santé, en la faisant passer des institutions vers eux même.

Certains auteurs parlent même de néo-libéralisme de la santé.[18] Les outils associés au mouvement du *quantified self* incitent en quelque sorte les individus à se voir comme des projets, à s'améliorer. Cela renvoie à un besoin constant d'aller toujours plus loin dans le développement de soi.

Le *quantified self* est devenu un moyen de se ré-approprier sa santé. Il est souvent fait le parallèle avec le phénomène du « pèse-personne ». Il est possible depuis longtemps de récolter les mêmes données que celles amassées via des dispositif adéquats. Cependant, cela devait se faire au sein des institution hospitalières. Le mouvement, quant à lui, innove en ce qu'il a rendu la récolte de ces données accessible au public. Tout comme lorsque la balance est passée du bureau du médecin vers la salle de bain du public.[19]

---

[15] V. LEE, « What's Happening in the "Quantified Self" Movement ? », in *Instructional Technology and Learning science Faculty publications,* 2014*,* Utah*,* n°491, pp. 1032 et s.

[16] V. LEE, *Ibid.,* p. 1032.

[17] D. LUPTON, « Quantified sex : a critical analysis of sexual and reproductive self tracking using apps », in *Cult Health sex*, 2014, n°17, pp. 1 à 14.

[18] P. DE SOUZA, Self-tracking and body hacking: The biopolitics of the Quantified Self in the age of neoliberalism, https://bodycartography.wordpress.com/2013/06/11/self-tracking-and-body-hacking-the-biopolitics-of-the-quantified-self-in-the-age-of-neoliberalism, consulté le 17 mars 2019 ; KELLY, K., dans TAKASHI D., Quantifiying our lives will be a top trend in 2012, article en ligne, disponible sur « https://venturebeat.com/2012/01/21/quantifying-our-lives-will-be-a-top-trend-of-2012/ », consulté le 13 mars 2019.

[19] K. CRAWFORD, Our metrics, ourselves: A hundred years of self- tracking from the weight scale to the wrist wearable device, 2015, *Eur J Cultural Studies,* pp. 18 et s.

§3 Le quantified self en quelques chiffres

A. Le marché

En plus d'être un mouvement, le *quantified self* est également un marché fructueux pour de nombreuses entreprises.

Ce marché est sujet à une très forte croissance. En effet, selon une recherche de la BCC d'un chiffre d'affaires total d'1,1 millard de dollars en 2013,[20] à 3,2 millards en 2014. Aujourd'hui, en 2019, on estime le marché à environ 14 millards de dollars. Les prédictions le placent aux alentours de 23 millards de dollars à l'horizon 2023.[21]

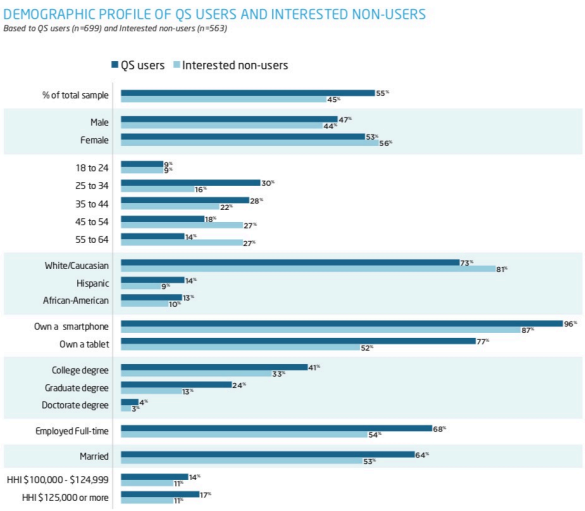
Malgré un croissance moyenne en baisse, de 6,1%/an en 2019 à 3,3%/an, en 2023, on estime que le marché a encore de beaux jours devant lui.

En ce qui concerne le nombre d'utilisateurs, on répertorie actuellement 390 millions d'utilisateurs dans le monde.

En 2014, Rocket Fuel, un service de développement d'intelligence artificielle, a réalisé une étude sur le profil des utilisateurs de *quantified self* habitant sur le sol américain. Ils ont découvert qu'environ 31% des américains déclarent traqueurs des données biométriques. La tranche d'âge la plus représentée est celle des 25 - 34 ans, regroupant plus de 30% des utilisateurs. Une des découvertes les plus importantes de l'étude est que 90% des sondés ressentent un effet bénéfique du *quantified self* sur leur capacité à atteindre leurs objectifs ou leurs performances physiques.[22]

---

[20] BCC Research, *Mobile Devices Driving Unprecedented Growth in Self-Monitoring Technologies Markets*, 2015.
[21] Statistiques de Statista : disponible à l'adresse : « https://www.statista.com/outlook/319/100/wearables/worldwide#market-marketDriver », consulté le 13 mars 2019.
[22] Statistiques de Statista : disponible sur : https://www.statista.com/outlook/319/100/wearables/worldwide#market-marketDriver, consulté le 13 mars 2019 ; Rocket fuel, *"Quantified Self " digital tools a cpg marketing opportunity*, 2014, p. 4, disponible en ligne à l'adresse : « http://quantifiedself.com/docs/RocketFuel_Quantified_Self_Research.pdf », consulté le 21 mars 2019.



Profil démographique des utilisateurs du quantified self et des non-utilisateurs intéressés

Il est également possible de se baser sur d'autres chiffres tels que le nombre de personnes inscrites au sein de groupes "*Meetup*", une plateforme de groupes en ligne. C'est par ce biais que se sont initialement rejoint les adeptes de réunions "*Show and Tell*".[23] Ces adeptes particulièrement impliqués sont plus de 90.000, repartis sur toute la planète au sein de 227 groupes.

Carte mondiale des groupes Meetup avec un intérêt pour le quantified self

[23] N. BERMINGHAM-MCDONOGH, *The data science of the quantified self*, 2015, Vrije Universiteit Amsterdam, p. 8.

B. Modèle économique et prix moyen

En ce qui concerne les prix d'utilisation du *quantified self*, il n'existe pas de travaux. La présente section est donc le fruit de nos propres recherches. Cette analyse se scinde en deux, d'une part, les traqueurs et de l'autre, les applications.

i. Les traqueurs

Les traqueurs sont généralement divisés en deux parties : les montres connectées et les bracelets d'activité. La différence majeure entre les deux réside dans la taille de l'écran mis à disposition de l'utilisateur, plus grand dans le cas de la montre.

À gauche, la montre Garmin Fenix - À droite, le bracelet FitBit Inspire

Le paiement pour ces outils est qualifié d' "*upfront"*, c'est-à-dire que l'utilisateur paie pour l'entrée en possession du produit, ce qui les différencie des applications.

En ce qui concerne les montres, le prix est compris entre 250 et 700€ chez Suunto,[24] entre 250 et 1500€ chez Garmin,[25] entre 150 et 300€ chez FitBit[26] et de 430 à 800€ chez Apple.[27]

En moyenne, il faudra compter environ de 250€ pour une montre d'entrée de gamme, aux alentours de 400€ pour un milieu de gamme et plus de 700€ pour des montres haut de gamme ou de luxe.

---

[24] Disponible à l'adresse : « https://www.suunto.com/fr-fr/Recherche-de-produits/Voir-toutes-les-montres-de-sport/ », consulté le 27 mars 2019.
[25] Disponible à l'adresse : « https://buy.garmin.com/fr-BE/BE/c10002-p1.html », consulté le 27 mars 2019.
[26] Disponible à l'adresse : « https://www.fitbit.com/nl/versa », consulté le 27 mars 2019.
[27] Disponible à l'adresse : « https://www.apple.com/fr/shop/buy-watch/apple-watch », consulté le 27 mars 2019.

Ces différences conséquentes de prix s'expliquent par les fonctionnalités et options mises à disposition de l'utilisateur. Un écran plus grand, du verre résistant aux éraflures, un bracelet dans un matériaux plus noble, une fonction cellulaire, c'est-à-dire une connexion 4G directement au sein de la montre, ou encore un modèle plus récent, sont des caractéristiques de nature à faire grimper le prix de ces montres.

Acquérir un bracelet coutera entre 70 et 140€ chez Garmin, 45€ chez Moov,[28] 130€ chez Withings,[29] de 100 à 150€ chez FitBit.

Il en coûtera une centaine d'euros à celui qui voudra se procurer un bracelet connecté.

ii. Les applications

Le schéma de prix est ici organisé différemment : le paiement ne se réalise que rarement à l'entrée. La majorité des applications prévoit un système basé sur le modèle du *Freemium*.

Application	Prix d'achat	Prix Prémium
Strava	Gratuit	60-80$/an
Runkeeper	Gratuit	40$/an
MyFitnessPal	Gratuit	50$/an
SleepCycle	Gratuit	30$/an
Runtastic	Gratuit	50€/an
Formyfit	Gratuit	100€/an

Né de la contraction entre les mots "*Free*" et "*Premium*", le modèle du *Freemium* est un modèle assez répandu dans le milieu des applications mobiles. Son principe est assez simple : une application se voit disponible sur un *store* de façon totalement gratuite, ce qui est généralement assez bien perçu des utilisateurs car ceux ci sont habitués à la gratuité sur internet.[30] Dans sa version gratuite, ses fonctionnalités se voient limitées et dans certains cas des publicités sont imposées.

---

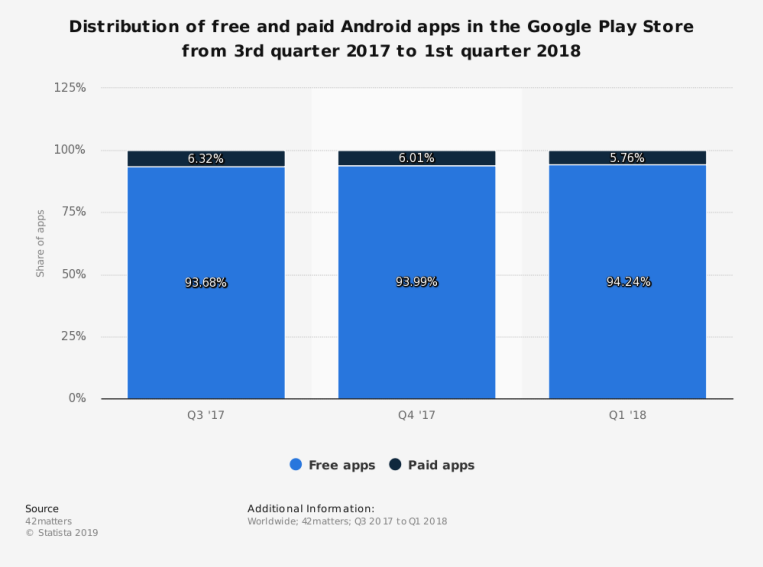
[28] Disponible à l'adresse : « https://store.moov.cc/products/moov-now », consulté le 27 mars 2019.

[29] Disponible à l'adresse : « https://www.withings.com/be/fr/pulse-hr », consulté le 27 mars 2019.

[30] P.-E. GOBRY, *Explainer: What Is The Freemium Business Model?*, 2011, disponible à l'adresse : « https://www.businessinsider.com/what-is-the-freemium-business-model-2011-4?IR=T », consulté le 27 mars 2019. Cela constitue donc généralement un bon atout marketing.

Dès lors, afin de se débarrasser de ces publicités et de pouvoir avoir accès aux fonctionnalités complètes de l'application, l'utilisateur en question devra mettre la main à la poche. Il existe généralement deux modèles de paiement pour ce type d'application. Soit "*Lump Sum*" c'est-à-dire que l'utilisateur paie une somme déterminée pour avoir accès à toutes les fonctionnalités de façon définitive, soit "*Running*" c'est à dire que l'utilisateur paie une somme mensuelle, trimestrielle ou annuelle afin de pouvoir avoir accès à la totalité de l'application.[31]

De façon générale, les statistiques prouvent que les applications mobile sont majoritairement gratuites, suivant ce modèle du *Freemium*.[32]



Proportion de téléchargements entre les applications payantes (en foncé sur le tableau) et gratuites (en clair sur le tableau) à l'entrée.

Cette stratégie semble naturelle de la part des entreprises développant des applications de *quantified self*. En effet, ce modèle a pour avantage de ne pas mettre de barrière à l'entrée et d'obtenir plus d'argent de la part des utilisateurs prêts à y mettre le prix.

Monsieur BAIJOT nous explique qu'ils ont quelques difficultés à communiquer sur cet aspect de l'application. La plus value de leur application résidant dans le *coaching*, qui est la dimension prémium de l'offre, leurs efforts publicitaires s'y concentrent. Dès lors de nombreux utilisateurs ne

[31] V. KUMAR, « Making Freemium Work », *Harvard Business Review*, 2014, disponible à l'adresse : « https://hbr.org/2014/05/making-freemium-work », consulté le 27 mars 2019.
[32] Disponible à l'adresse : « https://www.statista.com/statistics/266211/distribution-of-free-and-paid-android-apps/ », consulté le 27 mars 2019.

comprennent pas que la dimension *tracking*, qui est la partie gratuite de l'application, le restera toujours.

iii. L'expansion vers le business to business

Il nous explique également que son application a dû se développer dans deux directions pour pouvoir être viable. En premier lieu, l'application s'est développée dans un modèle *business to consumer*, c'est-à-dire que par une publicité adéquate et une bonne application, ils se voyaient déjà avec de nombreux utilisateurs dans le monde. Cela n'a pas été le cas. Même si les consommateurs restent une partie importante de leur public, il était nécessaire de voir plus large afin d'assurer la viabilité de l'entreprise.

Dans un second temps, *Formyfit* a diversifié son public cible en s'adressant également aux entreprises. Ils traitent directement avec les entreprises plutôt que les consommateurs. Cette collaboration prend généralement place dans le cadre d'un plan santé. Les clients personne morale vont payer un forfait à *Formyfit* pour que leurs employés puissent utiliser pleinement l'application. Cette formule comporte de nombreux avantages pour les deux parties. D'une part, les clients *business* achètent une formule relativement innovante qui permet de promouvoir la santé au sein de leur entreprise et d'autre part, les distributeurs de l'application possèdent un nouveau canal de vente au sein duquel il n'est pas nécessaire de faire de la publicité.

On peut voir dans ce modèle business to business, un nouveau marché pour le *quantified self* qui est celui de la santé au sein des entreprises.

Section 2. Le quantified self en pratique

Afin de pouvoir cerner au mieux du propos qui va suivre, il est nécessaire de comprendre ce qu'est le *quantified self*. Nous allons donc présenter successivement plusieurs applications et traqueurs dans le but d'expliciter au mieux ce type de pratiques.

Le *quantified self* peut se décliner sous plusieurs formes. Nous étudierons tout d'abord le cas des applications sur téléphone pour ensuite passer à l'analyse des différents traqueurs existants. Il est à noter que, malgré leur dissociation théorique, les deux se complètent.

Sous-Section 1. Les outils du quantified self

Il existe une diversité extraordinaire d'applications permettant de quantifier ce que nous voulons. Elles peuvent être réparties selon plusieurs thématiques comme le sport, le sommeil, ou encore l'humeur. Au sein de chacune d'elles nous allons détailler le fonctionnement en étayant au moyen de quelques exemples.

§1 Les applications automatisées

Cette catégorie d'applications[33] concerne tous les programmes qui récoltent des données sans que l'utilisateur ne doive rentrer les données manuellement. Le logiciel en question va récolter automatiquement les données par le biais des capteurs présents dans le téléphone (accéléromètre, altimètre,…) ou en collaboration avec un traqueur (rythme cardiaque, profondeur du sommeil,…).[34]

A. Le sport

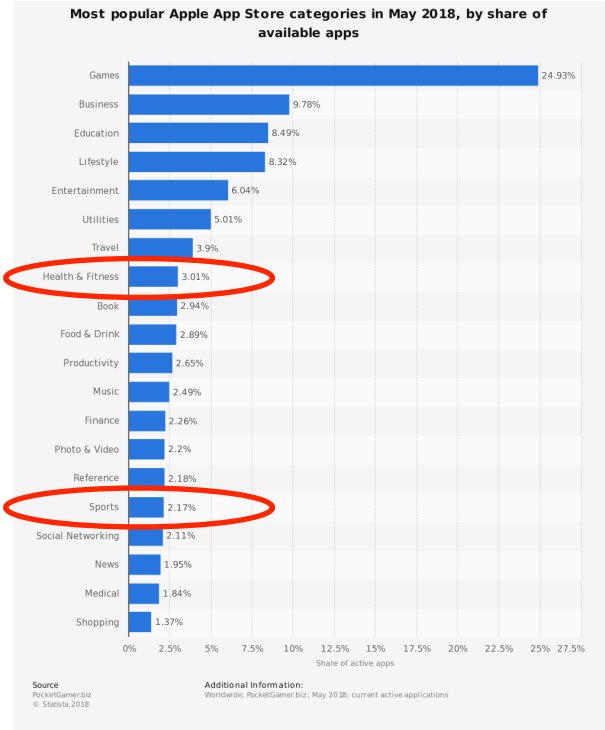
Les applications de sport sont des applications mobiles ayant pour objet de récolter des données à propos d'une activité sportive.

---

[33] B. BATHELOT, La définition d'une application mobile, 2017, disponible sur : https://www.definitions-marketing.com/definition/application-mobile/, consulté le 17 mars 2019.
Une application est : « […] un programme téléchargeable de façon gratuite ou payante et exécutable à partir du système d'exploitation d'un smartphone ou d'une tablette. »

[34] A. HILTS, C. PARSONS, ET J. KNOCKEL, *Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security*, Open Effect Report, 2016, p. 5, disponible sur : https://openeffect.ca/reports/Every_Step_You_Fake.pdf, consulté le 17 mars 2019.

Celles-ci sont les plus représentées dans le domaine du *quantified self*. En effet, comme l'illustre ce graphique, les applications concernant la santé et le sport représentent en tout presque 5% des applications téléchargées sur tout l' Apple Store en mai 2018.[35]



Catégories d'applications les plus populaires sur l'Apple Store en mai 2018

Les applications de sport peuvent être utilisées seules, c'est à dire que le téléphone va servir lui même de capteur afin de traquer l'activité (comme lorsque l'on utilise uniquement l'application Strava ou Runtastic) ou avec un traqueur externe au téléphone qui pourra venir s'appairer au téléphone. Les applications permettent de suivre une course à pied afin de déterminer les différentes performances accomplies durant l'entrainement.

Prenons l'exemple de l'application Strava,[36] une application développée par Strava INC, qui a pour objet de permettre aux athlètes pratiquant soit la course à pied, soit la natation, soit le cyclisme, d'enregistrer leurs performances.

Nous prendrons ici volontairement l'exemple de la course à pied.

---

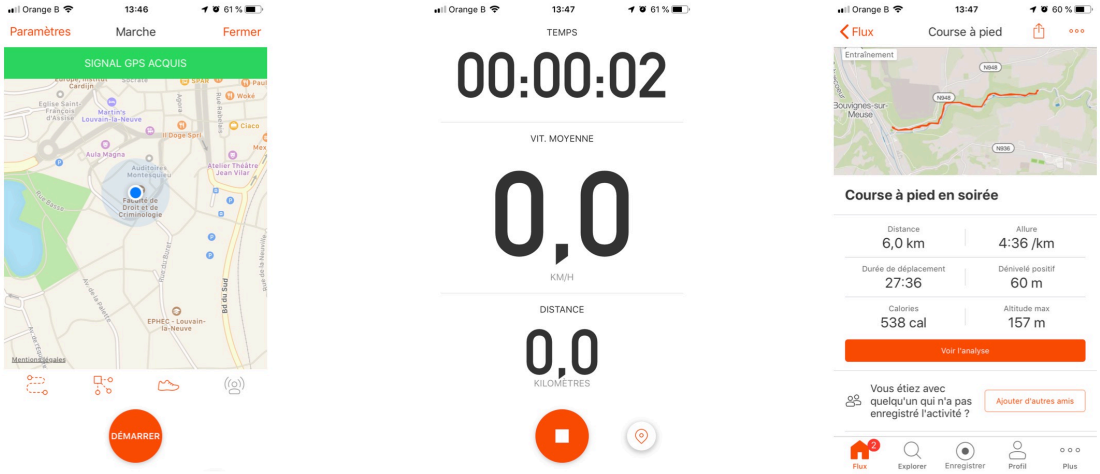
[35] Voy. : https://www.statista.com/statistics/270291/popular-categories-in-the-app-store/, consulté le 12 février 2019.
[36] Voy. : https://www.strava.com/, consulté le 12 février 2019.

En premier lieu, le sportif doit d'abord télécharger l'application sur le store de son choix, Android ou Apple en fonction de son modèle de appareil. Il a donc au préalable dû accepter la politique de vie privée de son appareil.

Ensuite, il doit lancer l'application téléchargée pour s'inscrire. Toute inscription engendrera automatiquement une acceptation de la politique de confidentialité de la dite application.[37] Nous reviendrons sur ces politiques plus tard dans notre propos.

Lorsque ces trois opérations sont réalisées, il suffit de lancer l'application qui propose au coureur d'enregistrer sa course (photo 1). Ensuite, durant la course, le coureur peut consulter en temps réel ses performances au moyen de l'écran. Il est averti, en plus, tous les kilomètres de sa cadence (photo 2). Enfin, après la course, le coureur peut consulter ce qu'il a accompli via un récapitulatif (photo 3), qu'il pourra directement publier depuis l'application vers différents réseaux sociaux.[38]

L'ensemble de ses performances sera affiché comme une sorte de journal qui lui permettra de consulter son évolution ainsi que sa régularité.



Captures d'écran au sein de l'application Strava : récapitulatifs de course

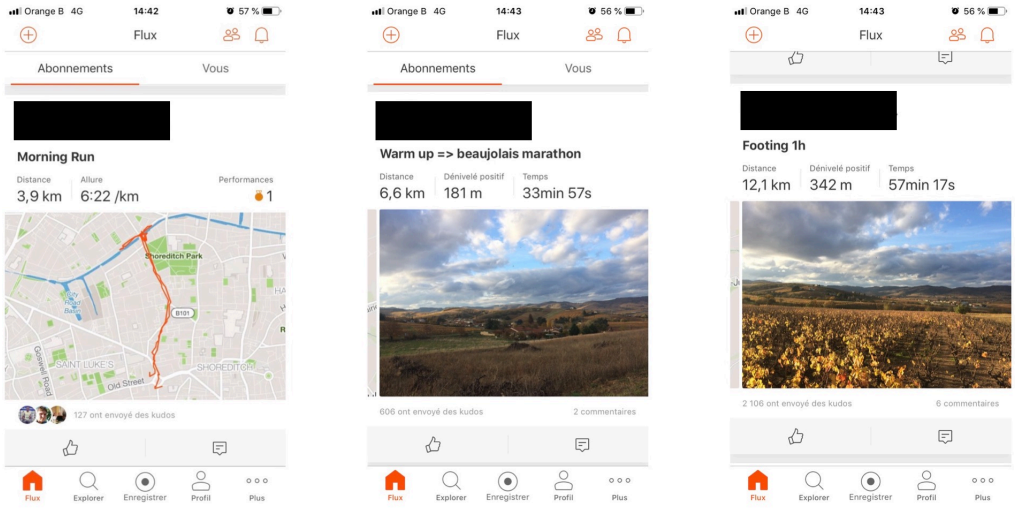
En plus de se comporter comme un traqueur d'activité, l'application se comporte également comme un réseau social autour du thème du sport.

---

[37] Pour la politique de confidentialité de Strava, voy. : https://www.strava.com/legal/privacy?hl=fr-FR, consulté le 12 février 2019.

[38] Photos personnelles, réalisées à partir de notre propre application.

Comme le montrent les photos suivantes, il est possible de suivre les activités et performances d'autres sportifs. À partir du moment où chacun publie ses activités sur son profil, n'importe qui faisant partie du réseau d'utilisateurs peut aller les consulter sauf si l'utilisateur fait lui même le choix de limiter l'accès à son profil pour les personnes qu'il choisi.



Activités partagées par des utilisateurs

Il existe également un système de récompenses pour les meilleurs entrainements basé sur des distances ou des temps bien définis, par exemple, le meilleur temps pour 10 kilomètres, le meilleur temps sur un segment défini, le meilleur temps pour accomplir un semi marathon, ou encore le plus grand nombre de kilomètres réalisés sur un mois.

Il existe également d'autres applications de course à pied, notamment une développée en Belgique dénommée *Formyfit*, avec le fondateur de laquelle nous avons eu la chance de nous entretenir. Cette application monte encore d'un cran dans le suivi.

En effet, plutôt que de se baser uniquement sur des données telles que le rythme de course, grâce à des données telles que le poids et le sexe de l'utilisateur, elle va calculer, grâce à un test précis réalisé par l'utilisateur, une estimation de la vitesse maximale aérobie (VMA) de laquelle elle extrapolera la VO_2 Max. Grâce à ces données, l'application va pouvoir mettre en place pour ses utilisateurs *premium*, un plan d'entraînement personnalisé en fonction de leurs capacités physiques. C'est donc un moyen d'aborder le sport d'une manière plus personnalisée. L'application va elle-

même construire des séances précises ainsi qu'un calendrier d'entrainement à l'utilisateur lui permettant d'atteindre les objectifs qu'il s'est fixé.[39]

À notre connaissance, *Formyfit* est la seule application à proposer ce type de tests, selon Monsieur BAIJOT, cela s'explique notamment par la difficulté de mettre ce type de technologie en place et par le peu de fiabilité qu'offrent les traqueurs servant à calculer les données servant de base à l'élaboration du plan.[40]

Il existe de nombreuses applications et les services qu'elles offrent sont généralement similaires à part *Formyfit* qui propose ce système de *coaching*. On peut dès lors s'attendre à une évolution des applications concernant le sport vers une dimension plus personnalisée.

B. Le sommeil

Les applications concernant le sommeil ont aussi contribué à l'essor du mouvement et sont, en quelque sorte devenues un phénomène de société. En effet, beaucoup de personnes en quête d'un meilleur sommeil se sont tournées vers les applications sur smartphones afin d'analyser leur sommeil pour trouver les causes de leurs troubles.

Certaines de ces applications peuvent être utilisées avec ou sans matériel supplémentaire tel qu'un bracelet ou une montre connectée. Elles ont pour but de calculer les périodes qu'une personne passe au lit, combien de temps celle-ci est endormie, quels cycles de sommeil elle traverse,…

Récapitulatif du sommeil de l'utilisateur

[39] Interview L. BAIJOT, Annexe, Question 1.
[40] *Ibid.,* Question 12.

Ici, ce qui est remarquable, c'est que l'on n'est pas dans une dynamique de comparaison avec l'autre. L'usage des données récoltées est destiné uniquement au traitement exclusivement privé de l'utilisateur. Il s'en sert pour pouvoir comprendre et adapter son sommeil de manière à l'améliorer pour un mieux-être général. En effet, vouloir mieux dormir que son voisin n'aurait que peu de sens.

Par contre, ce que l'on retrouve, comme dans les autres formes de *quantified self*, c'est cette forme de journal qui permet à l'utilisateur de suivre sa progression globale dans le but final d'accomplir son objectif, qui est de dormir le mieux possible.

Il n'y a donc ici aucun rapport avec la communauté. Le *quantified self* retrouve alors sa forme la plus simple telle la maxime d'un des fondateurs du mouvement : « *You can't improve what you can't measure* ».[41]

§2 Les applications manuelles

Contrairement à leurs homologues automatisées, ces applications visent à mesurer des données qu'il n'est pas possible de récolter via des capteurs. En effet, reporter son humeur ou ce que l'on a mangé n'est pas possible de manière automatique. Il sera obligatoire pour l'utilisateur de rentrer manuellement les données nécessaires au sein de l'application.[42]

A. L'alimentation

Nous allons ici prendre pour exemple l'application MyFitnessPal,[43] leader incontesté dans le domaine du suivi de l'alimentation. Le but de l'application est assez simple, elle permet à l'utilisateur de compter le nombre de calories ingérées dans la journée.

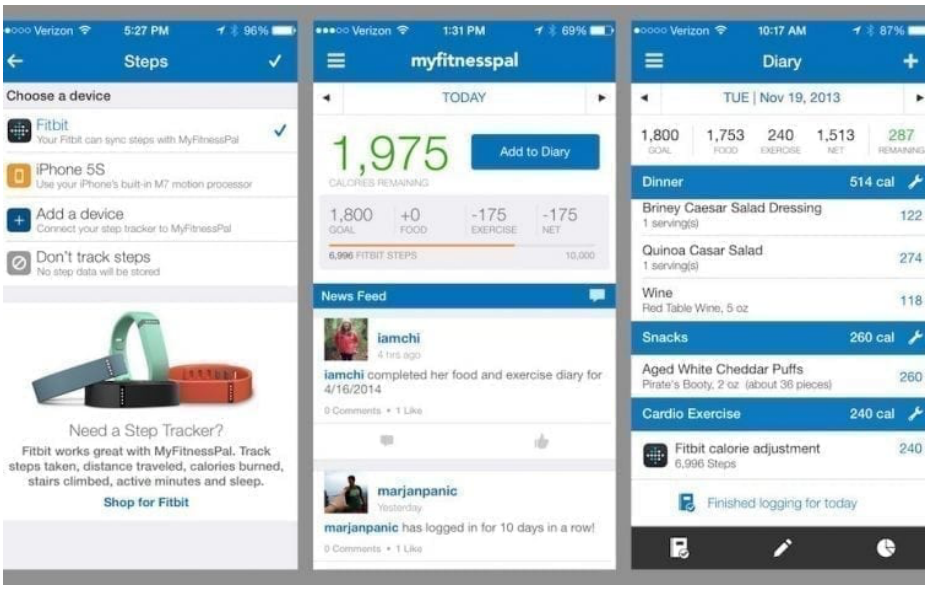
Pour ce faire, l'utilisateur de l'application doit entrer tour à tour l'ensemble des aliments qu'il mange durant sa journée. Chacun de ces aliments a un nombre de calories défini par l'application. Une simple addition fera ensuite l'affaire et permettra à n'importe qui souhaitant encoder ses aliments de connaître le total de l'apport calorique de sa nourriture.

---

[41] G. WOLF, « The data driven life », *The New York Times Magazine*, 2010, disponible en ligne à l'adresse : « https://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html », consulté le 20 mai 2019.
[42] A. HILTS, C. PARSONS et J. KNOCKEL, *Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security*, *op. cit*., p. 5.
[43] Voy. : https://www.myfitnesspal.com, consulté le 13 février 2018.

Afin d'atteindre ses objectifs, un athlète devra veiller à contrôler son alimentation. Cet outil offre le support nécessaire pour un suivi complet.[44] Il permet également de savoir quelle proportion de macro nutriments (glucides-lipides-protéines) sont ingérés quotidiennement par l'utilisateur. Ces données permettent donc aussi à quelqu'un souhaitant rééquilibrer son alimentation de connaitre les valeurs de chaque aliment.

La plus value qu'octroie ce genre d'application réside dans sa base de données. En effet, il est tout à fait possible de prendre un carnet chez soi dans lequel on consignerait chaque aliment ingéré. Cependant, l'application, elle, connait la valeur nutritionnelle de chaque aliment ce qui lui donne une réelle plus value par rapport à tout autre méthode. Il n'est dès lors plus nécessaire de recourir à un professionnel pour pouvoir calculer ces éléments basiques.[45]



Interface de l'application MyFitnessPal

B. L'humeur

Un autre type d'application du *quantified self*, moins connue, concerne l'humeur. Un exemple est "MoodPanda". Cette application permet à ses utilisateurs de consigner son humeur à n'importe quel instant. Chacun peut ainsi savoir quand il est le plus heureux et quand il se sent le mieux.

---

[44] B. AJANA, « Digital health and the bio politics of the quantified self », *op. cit.*, p. 3.
[45] Images : Voy. https://blog.myfitnesspal.com/now-you-can-track-your-steps-in-myfitnesspal/, consulté le 13 février 2019.

Ce type d'application est bien évidemment une niche, peu de personnes y prêtant de l'attention. Toutefois, elle nous montre que le *quantified self* offre des possibilités qui vont au delà du physique et peut également concerner la dimension psychologique.

Consigner chacune de ses humeurs à des moments variés a pour avantage de pouvoir identifier les périodes où l'on se sent le moins bien. En identifiant ces moments, il devient alors possible de réagir méthodiquement afin de remédier à ces instants de mal-être.

L'utilisateur, s'inscrit et crée un profil pseudonymisé. En effet, seule la première lettre de son nom de famille est dévoilée. Ainsi, au regard de la communauté, il n'est pas possible d'identifier qui se trouve derrière tel profil. On remarquera cependant qu'au regard de la législation concernant les données personnelles, ce type de données doit être considéré comme personnelle.[46]

Cet utilisateur dispose donc d'une interface au travers de laquelle il peut évaluer quotidiennement comment il se sent sur une échelle de 1 à 10. Il peut également accompagner cette note d'un commentaire explicitant la raison de son humeur. Par exemple, un utilisateur ayant atteint son objectif de perte de poids pourra l'indiquer afin de commenter sa note de 9/10 alors qu'un autre pourra expliquer sa note de 1/10 par le fait que sa voiture a été emboutie.

Cette appréciation est alors publiée et visible parmi les membres et utilisateurs de l'application. N'importe qui peut dès lors entrer en discussion avec celui qui a posté son état d'humeur pour, par exemple, essayer de le réconforter ou en apprendre plus sur elle/lui.

MoodPanda est également une application particulière car elle ne repose pas sur le modèle *freemium*. En effet, l'ensemble des fonctionnalités sont gratuites. Les coûts de fonctionnement sont financés par les dons de généreux donateurs. Afin de les remercier, l'application met en place un système de badges afin de reconnaitre les personnes qui font vivre l'application.

Cette application met en lumière une autre dimension, moins développée par les autres, qui est l'appel à la communauté. En effet, ici, la dynamique de l'application est bien différente, on y renverse le paradigme de telle sorte que ce ne sont pas les performances postées par l'individu qui sont intéressantes mais toute la communauté de support autour.

[46] Article 4.1 du RGPD

§3 Les traqueurs

Le phénomène du quantified self s'est développé autour d'une volonté du public de retracer les activités du corps en les quantifiant afin d'avoir un effet positif sur son bien-être.[47]

Ces pratiques, bien que peu récentes,[48] se sont démocratisées lors de la prolifération des traqueurs numériques d'activité.[49] Auparavant, tout ce qui concernait la mesure de soi passait par des outils manuels tels qu'un cahier ou un podomètre. Aujourd'hui, tout est automatique et passe par ces dispositifs.

Un traqueurs d'activité est défini par MATTHEW B. HOY comme un "appareil électronique" présentant les trois caractéristiques suivantes :

« (1) est spécialement conçu pour être porté sur le corps de l'utilisateur;

(2) utilise des accéléromètres, altimètres, ou d'autres senseurs pour traquer les mouvements et/ou les données biométriques de l'utilisateur;

(3) et envoie les données de l'activité vers une application en ligne qui montre la tendance dans le temps. »[50]

Il existe une pléthore d'appareils pouvant être qualifiés de traqueurs numériques. Alors que certains sont expressément développés dans ce but comme les FitBit Charge, Moov, Apple Watch, Xiaomi Band,…[51] D'autres, ont misé sur les capteurs présents dans la majorité des smartphones pour nourrir leurs applications telles que Strava, Runtastic ou encore Nike+…[52]

L'analyse du *quantified self* ne peut se limiter aux seules applications. En effet, les capteurs qui y sont généralement associés sont partie prenante dece mouvement. Il en existe un nombre incalculable sous des formes très diverses. Ces capteurs peuvent prendre la forme d'une ceinture thoracique contrôlant le rythme cardiaque, d'une brassard contrôlant la pression du sang, d'une

---

[47] B. AJANA, « Digital health and the bio politics of the quantified self », *op. cit.*, p. 2.
[48] B. AJANA, *Ibid.,* p. 3.
[49] M. HOY, *Personal activity trackers and the Quantified Self,* Eau Claire, 2016, Vol. 35, n°1, p. 94.
[50] M. HOY, *Ibid.,* p. 95.
[51] Pour ces traqueurs, voy. not. : https://www.fitbit.com/fr-ca/charge3, https://welcome.moov.cc, https://www.apple.com/fr/watch/ et https://www.mi.com/global/miband/, consultés le 19 février 2019.
[52] Pour ces applications voy. not. : https://www.strava.com, https://www.runtastic.com/fr/, http://moodpanda.com et https://www.myfitnesspal.com, consultés le 19 février 2019.

montre contrôlant aussi bien l'activité que le nombre d'heures passées debout ou encore d'un simple petit bracelet, aussi connecté que discret.

Chaque type de capteur a ses particularités et sa cible en terme de consommateurs. Ils proposent chacun des fonctionnalités les plus diverses. Nous allons en analyser deux, assez populaires afin de donner un aperçu de ce type de technologie.

A. L'Apple Watch

L'Apple Watch est ce que l'on appelle une montre connectée. Une montre connectée, aussi appelée en anglais *smartwatch* est : « une montre électronique qui intègre des fonctions de communication élaborées : réception-émission d'appels téléphoniques, notifications provenant d'un téléphone mobile, envoi et réception de messages, reconnaissance vocale. Ces instruments sont la plupart du temps équipés d'un écran tactile qui permet de personnaliser l'affichage en changeant le cadran ; en général, ils font office de compagnon pour les smartphones auxquels ils sont associés par liaison Bluetooth ».[53]

L'Apple Watch a été commercialisée en 2015 et n'a cessé d'évoluer depuis. On l'appelle montre car elle ressemble à une montre, c'est-à-dire qu'elle a un cadran ainsi qu'un bracelet et elle se porte au poignet. Elle est pourtant bien plus que cela. C'est une sorte de petit ordinateur, connecté à notre téléphone et portée au poignet, permet en plus de donner l'heure, de lire des sms, recevoir ses notifications de mails,…

En plus de tout cela, l'Apple Watch permet également, grâce à son capteur placé sous le cadran, de relever des données corporelles telles que le rythme cardiaque, ce qui lui permet d'estimer le nombre de calories dépensées (rond rouge sur l'image) tout au long de la journée, d'établir une courbe du rythme cardiaque à court, moyen ou long terme… Elle affiche également le nombre d'heures durant lesquelles nous avons été debout (rond bleu sur l'image) et enfin le nombre de minutes d'activités dans la journée (rond vert sur l'image).

Chacun de ces cercles est représentatif d'un objectif à atteindre durant la journée et cela tous les jours de l'année. Le cercle bleu fixe pour objectif de rester debout au moins une minute chaque heure et cela 12 fois par jour, le vert de pratiquer 30 minutes d'activité et le rouge, paramétrable par

---

[53] Futura Tech, Définition d'une montre connectée, disponible sur : https://www.futura-sciences.com/tech/definitions/montre-intelligente-montre-connectee-15456/, consulté le 17 mars 2019.

l'utilisateur au gré de ses préférences, lui permet de se donner un objectif quotidien de dépense calorique. Le tout est retransmis en direct sur le téléphone de l'utilisateur.

Les objectifs "bleu" et "vert", sont des objectifs par défaut et sont immuables. En effet, ceux-ci se basent sur des bienfaits communément admis : se tenir régulièrement debout[54] et pratiquer une activité physique régulière, comme par exemple 30 minutes de marche par jour.[55]

L'objectif rouge, quant à lui, concerne l'objectif de calories à dépenser par jour et est librement paramétrable par l'utilisateur. Il pourra ainsi décider de se fixer un objectif de 450 kilocalories ou de 750 kilocalories par jour, à dépenser via de l'exercice. En fin de semaine, le traqueur fait lui même un bilan hebdomadaire et invite, sur base des données récoltées durant la semaine précédente, à adapter ou non l'objectif en fonction des résultats réalisés. Par exemple, l'utilisateur qui n'atteint jamais la moitié de son objectif quotidien de dépense de calories sera invité à le baisser alors que celui qui le réalise a 200% chaque jour sera invité à l'augmenter.

Enfin, il existe un système de trophées (récompenses pour performances régulières ou extraordinaires) destinés à motiver l'utilisateur à se surpasser, ainsi qu'un système de partage permettant, comme dans les applications, de comparer ses performances avec les autres utilisateurs.

Performances sous forme de cercle

Performances sous forme de graphe

Trophées

[54] BBC News, « Calorie burner: How much better is standing up than sitting? », *BBC Website*, disponible en ligne à l'adresse : « https://www.bbc.com/news/magazine-24532996 », consulté le 9 avril 2019.
[55] Centre Canadien d'hygiène et de sécurité au travail, *La marche, toujours le meilleur remède*, disponible en ligne à l'adresse : « https://www.cchst.ca/oshanswers/psychosocial/walking.html », consulté le 9 avril 2019.

B. Le bracelet FitBit

Le bracelet FitBit est un autre accessoire assez connu sur le marché des capteurs. Plus petit et plus discret, il remplit en quelque sorte les même fonctions que l'Apple Watch examinée ci-dessus. On y retrouve de nombreuses similarités comme celle de pouvoir enregistrer ses sessions de sport, y examiner ses données telles que le rythme cardiaque, le nombre de calories brulées sur la journée,…

En raison de sa taille plus petite et à ses fonctionnalités plus limitées, le bracelet FitBit, n'intègre pas toutes les applications comme son homologue à la pomme.

Ce type d'appareil, également connecté au smartphone de l'utilisateur, dispose aussi d'une fonctionnalité permettant le partage des données à d'autres utilisateurs grâce, encore une fois, à une sorte de réseau social mis en place par la plateforme.

Ces objets sont donc globalement comparables et sont surtout une question de goût, d'affinités mais aussi d'interopérabilité, l'Apple Watch nécessitant un appareil sous iOS pour fonctionner.

Sous-Section 2. Les utilisations dérivées du quantified self et leurs risques

Les outils de *quantified self* ayant pour avantage de récolter des données à partir du moment où ils sont portés, intéressé d'autres secteurs. Notamment, les assurances et la justice qui, au États-Unis, ont déjà fait usage de ces dispositifs.

§1 La justice

Dans les affaires de dommages corporels, les traqueurs peuvent se révéler de véritables atouts pour apprécier l'étendue d'un dommage, notamment dans une affaire qui s'est déroulée au Canada.

En effet, au sein d'une affaire de dommage personnel, une coach sportif a subi un dommage corporel conséquent au cours d'un accident. Dans ce genre d'affaires, pour obtenir une compensation du dommage subi, il est nécessaire de prouver la baisse d'activité de la victime liée à cet accident. Cependant, prouver ce type de dommage se révèle souvent assez hasardeux car il n'est pas possible d'obtenir des données pertinentes sur la différence entre l'état auparavant et l'état actuel, c'est-à-dire, l'état après l'accident. Les décisions se basaient donc principalement sur des diagnostics médicaux à posteriori.

C'est donc à cet endroit précis que le *quantified self* intervient. Malgré le fait que la coach sportif ne portait pas de bracelet connecté auparavant, il serait possible de prouver que sont taux d'activité actuel était nettement inférieur à celui d'un coach sportif.[56] Cette profession étant reconnue pour entretenir une condition physique irréprochable, un taux d'activité physique très bas relevé par un bracelet connecté pourrait alors servir de preuve pour soutenir l'existence d'un dommage devant donner lieu à une compensation.[57]

Malgré les avantages que peuvent offrir les outils du *quantified self*, il peuvent également se retourner contre leur propriétaire. Dans une affaire américaine, la police du Comté de Lancaster, en Pennsylvanie, a utilisé les données récoltées par un bracelet FitBit afin de prouver le mensonge d'une prétendue victime de viol. Celle-ci avait déclaré s'être réveillée étendue après avoir été victime de l'acte en question. Cependant, les policiers, grâce aux données de son bracelet, on pu prouver qu'elle était bel et bien en train de bouger durant toute la période où elle déclarait être inconsciente. Le bracelet a donc rendu sa plainte pour viol nulle.[58]

Le *quantified self* pourrait donc devenir un moyen alternatif d'apporter la preuve d'un dommage dans des cas particuliers, devenant ainsi une boite noire du corps humain.[59] Il n'existe cependant pas encore de cas similaire en Europe.

Cette utilisation n'est pas sans poser des questions quant à la fiabilité de ces données et aux obligations de sécurité.

§2 Les assurances

Depuis quelques années, certaines compagnies d'assurances se sont penchées sur le phénomène, notamment aux USA et au Royaume-Uni. Les compagnies Oscar[60] et Vitality[61] ont en effet la

---

[56] P. OLSON, « FitBit data now used in court room », Forbes, 2014, disponible à l'adresse : « https://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/#2862ec177379 », consulté le 30 mars 2019.

[57] K. VINEZ, « The Admissibility of Data Collected from Wearable Devices », *Stetson Journal of Advocacy and the Law, 2017*, p. 10, disponible à l'adresse : « https://www2.stetson.edu/advocacy-journal/wp-content/uploads/2017/06/Vinez_-_Wearables.pdf », consulté le 9 avril 2019 ; K. CRAWFORD, « When Fitbit Is the Expert Witness », *The Atlantic*, 2014, disponible en ligne à l'adresse « https://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936/ », consulté le 9 avril 2019.

[58] K. VINEZ, *Ibid*, p. 9. ; K. HILL, « FitBit data just undermined woman's rape claim », *SplinterNews,* 2015, disponible en ligne à l'adresse : « http://tinyurl.com/FitBitdatajustundermined », consulté le 9 avril 2019.

[59] J. NINI, « How Wearable Technology is Making It's Way into the Courtroom », *Smith Lawyers' Blog*, 2018, disponible à l'adresse : https://www.smithslawyers.com.au/post/wearable-technology-courtroom, consulté le 30 mars 2019.

[60] Site officiel de l'assurance Oscar : « https://www.hioscar.com/ny », consulté le 5 mai 2019.

[61] Site officiel de l'assurance Vitality : « https://www.vitalitygroup.com/how-vitality-works/ », consulté le 5 mai 2019.

particularité de proposer des plans d'assurance santé personnalisés sur la base de dispositifs de *quantified self*.

Toute une série de données récoltées par les assurés seraient donc transmises à l'assureur. Une activité sportive régulière aurait donc pour conséquence de réduire la prime d'assurances, ce qui aurait pour effet d'avantager les personnes en bonne condition physique. Il s'agit d'une avancée majeure dans le monde des assurances où les données ne seraient plus possédées par les assureurs mais par les assurés.[62]

Durant notre discussion avec Monsieur BAIJOT, nous avons discuté de la probabilité de l'émergence d'un tel modèle en Belgique. Selon lui, il est possible que des produits d'assurance couplés à un dispositif de *quantified self* se développe chez nous. Pour lui, il y a encore des progrès à faire dans la technologie employée, la seule dimension comportementale est trop manipulable. Nous avons par exemple discuté de la triche qu'il existe dans ce type d'applications et qui a déjà été décelée par les autres compagnies d'assurances comme le fait que quelqu'un d'autre fasse les exercices à la place de l'assuré ou de simuler les pas réalisés dans la journée grâce à son animal domestique,… De plus, il estime que le marché n'est pas encore prêt pour ce type d'innovations.[63]

Cependant, il reste de nombreux obstacles à la mise en place d'un tel système en Europe. La donnée personnelle, de surcroît sensible, étant au coeur de ce modèle économique, un vrai défi attend les compagnies d'assurances. En effet, elles devront se conformer à toutes les obligations notamment de stockage, de traitement, de restitution des données. Ce type de pratiques a donc très peu de chances d'arriver en Europe à cause de la législation sur les données personnelles.

Un indice de cette impossibilité réside au sein du considérant 54 *in fine* du règlement européen sur la protection des données de 2018. Il dispose que dans aucune hypothèse, un traitement sans consentement pour motif d'ordre public ne pourra justifier une quelconque transmission de ces données à une compagnie d'assurances.

Il existe également un obstacle à ce type d'assurances en Belgique. La loi sur les assurances de 2014 en son article 58,[64] dispose qu'aucune donnée génétique ne puisse être communiquée aux

---

[62] B. ARRUABARRENA, *Le Soi augmenté : les pratiques numériques de quantification de soi comme dispositif de médiation pour l'action*, Sciences de l'information et de la communication, Conservatoire national des arts et métiers - CNAM, 2016, p. 208.

[63] Interview L. BAIJOT, Annexe, Questions 9 et 10.

[64] Loi du 4 avril 2014 relative aux assurances, *M.B.*, 30 avril 2014, article 58.

compagnies d'assurances. Cette disposition limite d'autant plus l'éventualité de voir apparaitre ce type de produit chez nous. Comme évoqué plus haut dans le cadre de la justice, il existe aussi de nombreux soupçons quant à la fiabilité des dispositifs utilisés.

Section 3. Analyse approfondie du mouvement

§1 Mesure et quantification

Avant tout, il nous semble nécessaire d'insister sur un point lexical qui est essentiel selon A. ROUVROY.[65] Au sein de son propos, elle explique qu'afin de comprendre la démarche, il est nécessaire de différencier les termes "quantifier" et "mesurer".

Le coeur de ce mouvement réside en une écriture en nombres de ce qui se passe à l'intérieur de notre corps. Nous sommes passés d'une époque où seules certaines données étaient mesurables, à une autre où tout devient quantifiable.[66]

Si quantifier consiste à « exprimer et faire exister sous une forme numérique ce qui, auparavant, était exprimé par des mots et non par des nombres » alors, « l'idée de mesure implique que quelque chose existe sous une forme déjà mesurable (...) comme la hauteur de la Tour Eiffel ».[67]

Le *quantified self* relève donc plus de la quantification que de la mesure, les notions de bonne santé, ou de bonne humeur n'étant pas des notions qu'il est possible de calculer en tant que tel.[68] Cependant, il est possible de les évaluer via une démarche de quantification.

Par exemple, il n'est pas possible de mesurer avec des données objectives l'humeur dans laquelle un sujet se trouve.[69] Pourtant, il pourra s'exprimer et évaluer son humeur sur une échelle subjective. C'est exactement la même chose que lorsqu'un médecin demande à un patient d'évaluer sa douleur, ce n'est pas mesurable mais quantifiable.

---

[65] A. ROUVROY, « Avant-Propos », *CNIL, Le corps, nouvel objet connecté, du quantified self à la m-santé : les nouveaux territoires de la mise en donnée du monde, Cahiers IP, n°2*, 2014, p. 4 disponible sur : https://www.cnil.fr/sites/ default/files/typo/documentCNIL_CAHIERS_IP2_WEB.pdf.

[66] E. BIRKAVS, M. KOEDIJK, X. MING et B. WOLBERS, *op. cit.,* p.2; Voy. aussi, A. ROUVROY, « Avant-Propos », *CNIL, Le corps, nouvel objet connecté, du quantified self à la m-santé : les nouveaux territoires de la mise en donnée du monde, op. cit.,* p. 4.

[67] A. DESROSIÈRES, « Pour une sociologie historique de la quantification », *L'argument statistique I*, 2008, Presses de l'École des mines, pp. 10 et 11.

[68] A. ROUVROY, « Avant-Propos », *CNIL, Le corps, nouvel objet connecté, du quantified self à la m-santé : les nouveaux territoires de la mise en donnée du monde, op. cit.,* p. 4.

[69] Voy. not. : http://moodpanda.com et http://www.moodscope.com, consultés le 18 février 2019.

La quantification est néanmoins plus large que cela et, dans le cadre de ce mouvement, elle implique le calcul de différentes données relatives au corps tel que les battements du coeur, le temps de sommeil, la durée d'une séance de sport,…

§2 La communauté

Au fil du temps, les applications de *quantified self* se sont développées et ont élargi le champ de leurs services. En effet, en plus de proposer des méthodes de quantification, elles se diversifient en proposant un réseau social intégré à l'application.

Cela fait en quelque sorte écho aux réunions "*Show and Tell*" organisées par le mouvement. Il existe au sein de la communauté un désir de partager.[70]

Plusieurs auteurs[71] semblent considérer que le concept même du *quantified self* ne peut être réduit au self lui-même. En effet, le rapport à la personne est souvent trop mis en avant par rapport à la communauté sous-jacente et ayant été fondamentale afin de créer le mouvement.

De façon générale, les applications intègrent de plus en plus au sein même de leur interface, des réseaux sociaux permettant aux utilisateurs de partager leurs quantifications.

Le Pr. AJANA[72] explique qu'il existe deux raisons pour lesquelles les utilisateurs s'adonnent à des pratiques de partage.

D'une part, on peut relever dans ce type de pratiques une forme d'encouragement et de reconnaissance de la part des autres utilisateurs. A contrario, la motivation peut aussi être dans la peur de décevoir cette même communauté : ne pas atteindre les objectifs fixés peut être un motivation à poursuivre un mode de vie sain.

D'autre part, l'auteur précise également que l'environnement mis en place par les applications peut être une cause de la volonté de partager. En effet, comme abordé plus tôt,[73] des applications mettent en oeuvre un système de récompenses. Ainsi, Strava propose une série de segments chronométrés

---

[70] N. DOW SCHÜLL, Self in the loop : « Bits patterns, and pathways in the quantified self », *The Networked Self*, 2018, New York, Vol 5: Human Augmentics, Artificial Intelligence, Sentience, Ed. Zizi Papacharisi p. 26.

[71] B. AJANA, « Digital health and the biopolitics of the quantified self », *Digital Health*, Londres, 2017, Vol. 3, p. 6. ; C. GICQUEL, P. GUYOT, *Quantified self, les apprentis sorciers du « moi connecté »*, Paris, FYP éditions, 2015, p. 107.

[72] B. AJANA, « Digital health and the biopolitics of the quantified self », *op. cit.*, p. 6.

[73] Voy. Sous-Section 1. Les outils du quantified self

sur lesquels les athlètes se défient pour obtenir le meilleur temps.[74] Les athlètes se défient sur des portions délimitées pour être le plus rapide et des récompenses virtuelles sont octroyées aux détenteurs des meilleurs chronométrages.

Illustration des différents trophées accumulables sur Strava

Malgré que l'idée de récompenser les meilleurs soit assez naturelle et favorise la fidélité à l'application, Monsieur BAIJOT nous explique que ce type de trophées possède des effets pervers.

Tout d'abord, cela donne une vision de la course à pied comme une éternelle compétition, comme si seulement la performance était la seule chose à atteindre dans tous les entrainements. C'est, selon lui, une vision erronée qui aura parfois pour conséquence de pousser les novices au delà de leurs limites, les écoeurant du sport alors que leur volonté était de se construire une meilleure santé.[75]

De plus, ces trophées attirent de nombreux tricheurs. De par son expérience, Monsieur BAIJOT nous confie qu'il existe de nombreux tricheurs au sein des ses applications. Il est édifiant de constater ce que les utilisateurs sont prêts à réaliser pour obtenir le meilleur rang possible en faisant le moins d'efforts. Il nous parle notamment de certains abus comme de courir avec plusieurs téléphone ou de la sur-utilisation des modes donnant accès à des points au sein de son application.[76]

En ce qui concerne le phénomène en général, il est appelé "gamification". Selon la synthèse des opinions réalisée par T. LECLERCQ et son équipe,[77] la définition la plus actuelle semble être celle de HUATORI et HAMARI : «[la gamification est] un processus d'amélioration d'un service avec des

[74] Image disponible sur : https://rennyrambles.wordpress.com/2015/03/23/strava-struck/, consulté le 27 mars 2019.
[75] Interview L. BAIJOT, Annexe, Question n°13.
[76] *Ibid*., Question n°10.
[77] T. LECLERCQ, I. PONCIN, W. HAMMEDI et A. KULLAK., *Effects of Gamification on Customer Engagement in Online Communities,* Louvain Research Institute in Management and Organizations Working Paper Series, 2018/10.

moyens financiers pour une expérience ludique afin de soutenir la création de valeur globale des clients ».[78] Selon eux, cette définition permet de mettre en balance les fonctionnalités imposées par les développeurs de l'application et le rôle du consommateur qui l'utilise.

Grâce à ces innovations, les consommateurs ne sont plus simplement des simples participants isolés, ils rentrent en compétition avec les autres utilisateurs. Ils deviennent membres à part entière de la communauté, s'y concurrencent et participent à son développement.[79]

Selon V. LEE, la participation au *quantified self* doit être considérée comme une espace d'affinité, cela « renvoie à une affiliation sociale organisée autour d'un projet commun qui implique des degrés variables de participation discrétionnaire et des échanges de connaissances multidirectionnels et hautement distribués dans divers médias. »[80]

Au delà de cette formulation un peu brumeuse, le concept d'espace d'affinités est souvent associé à l'exemple des jeux-vidéos et de leur communauté. En effet, on remarque qu'en l'absence du jeu vidéo comme une entité unique, il existe une communauté et toute une série de pratiques qui les entourent. On peut notamment citer les forums, les conventions,… Faire partie de ce monde va donc plus loin que de simplement jouer.

C'est tout à fait la même chose avec le *quantified self*. On retrouve en son sein, le fait de se quantifier mais aussi toute une série de pratiques annexes qui composent cet univers. On peut ici penser au site,[81] qui comprend notamment un forum, des news, aux rencontres *meet-up*,… Une facette non négligeable est également celle des réseaux en ligne créés par les applications elles-mêmes.

Peu importe la façon dont on le pratique, le *quantified self* devient un facteur de cohésion entre les individus qui se reconnaissent les uns les autres au sein de ces pratiques. C'est d'ailleurs ce qui a permis de former un mouvement.[82]

---

[78] K. HUOTARI,et J. HAMARI, « A definition for gamification: anchoring gamification in the service marketing literature », *Electronic Market*s, 2017, n°27/1, p. 25, traduction libre.
[79] M. MACIULIENE et A. SKARZAUSKIENE, « Evaluation of co-creation perpective in networked collaboration platforms », *Journal of Business Research,* 2016/69, pp. 4826 à 4830.
[80] V. LEE, « What's Happening in the "Quantified Self" Movement ? », *Instructional Technology and Learning science Faculty publications,* 2014*,* Utah*,* n°491, p. 1033.
[81] Site officiel du quantified self, disponible à l'adresse : « quantifiedself.com », consulté le 27 mars 2019.
[82] J. LAURENT, « Healthscapes of self-quantification : Quantifying, knowing and improving one's self: transforming health » *op. cit.*, p. 111.

Même si ces pratiques sont souvent perçues depuis l'extérieur comme narcissiques, elles sont en réalité teintées d'une réelle part de solidarité. Le *tracking* en lui même n'est plus seulement un moyen de se quantifier mais devient une passerelle vers les autres, au même titre que n'importe quel autre intérêt commun.[83]

Indiquons cependant que cette communauté n'est pas ouverte à qui le veut. Elle requiert naturellement la possession d'un dispositif de *tracking*. Elle présuppose donc un certain capital social et financier.[84]

[83] T. SHARON, *Self-tracking for health and the quantified self: Re-articulating autonomy, solidarity, and authenticity in an age of personalized healthcare*, 2016, Philos Technology, p.129.

[84] B. AJANA, « Digital health and the biopolitics of the quantified self », *op. cit.*, p. 8.

Chapitre 2. Les données personnelles et le quantified self

Introduction

En tant que mouvement basé sur la récolte de données, le *quantified self* est intrinsèquement lié à la législation applicable en matière de données personnelles. En effet, chacun des traqueurs ou des applications présentées ci-dessus ne pourrait fonctionner sans les données qui lui sont fournies. Qu'adviendrait-il d'un traqueur qui n'aurait aucune donnée à afficher à son utilisateur ?

Ces données sont transférées vers des responsables de traitement qui les traitent afin de pouvoir offrir des services de *quantified self* aux utilisateurs.

Cependant, elles ne sont pas à mettre entre toutes les mains. Elles ne doivent pas être traitées sans raison et doivent faire l'objet de garanties quant à leur utilisation. C'est donc pourquoi il est nécessaire de les encadrer en mettant en place un cadre législatif strict qui leur sera applicable. Cette matière est considérée comme un droit fondamental au regard des articles 8, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne et 16, paragraphe 1, du Traité sur le fonctionnement de l'Union européenne.[85]

Nous étudierons dans les sections à suivre le cadre législatif entourant les données traitées par les services de *quantified self*. Après un aperçu de l'environnement législatif, nous étudierions plus en profondeur les notions propres à la matière telles que le caractère personnel, le traitement, les obligations propres au responsable du traitement ainsi que les droits des personnes concernées. Ensuite, nous tacherons de donner au lecteur un aperçu des pratiques du mouvement afin d'évaluer leur conformité aux dispositions du RGPD.

[85] Considérant n°1 du RGPD.

Section 1. Le cadre législatif

La matière des données personnelles est relativement récente, elle a été implantée en Belgique via la loi du 8 décembre 1992[86]. Elle a été suivie de près par une directive européenne en 1995, dénommée ci-après : la Directive.[87] Cette législation a été le siège de la matière jusqu'au 25 mai 2018 et une partie non négligeable de celle-ci est encore d'application aujourd'hui. Notamment les notions de "traitement" et de "données à caractère personnel" restent semblables malgré quelques modernisations nécessaires.[88]

Cette directive a été remplacée par le règlement 2016/679, aussi appelé Règlement Général sur les Données Personnelles (RGPD).[89] Ce dernier a été publié au Journal Officiel de l'Union Européenne le 4 mai 2016 et est devenu applicable le 25 mai 2018. Il était nécessaire de laisser un délai raisonnable aux entreprises afin qu'elles puissent se conformer à leurs nouvelles obligations.

Le choix du règlement s'est imposé assez naturellement. En effet, eu égard aux disparités d'interprétation par les états membres dans la transposition de la directive, un instrument plus contraignant était nécessaire afin d'assurer une harmonisation forte. Cette harmonisation est considérée comme étant le meilleur moyen d'offrir la sécurité juridique et la transparence nécessaire aux acteurs présents sur le plan européen.[90]

En ce qui concerne le droit belge, le législateur a jugé utile de transposer les principes du règlement directement dans une loi. De là, est née la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.[91] Elle a notamment pour objet de préciser les sections du règlement laissées à l'appréciation du législateur national. Par exemple, ce qu'il convient d'entendre, en droit belge, lorsque le règlement désigne une autorité publique. Ou encore

---

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

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

88 DE TERWANGNE, C., « Titre 2 - Définitions clés et champ d'application du RGPD », *Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Éditions Larcier, 2018, p. 56.

89 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.*, L119 du 4 mai 2016, pp. 1 à 88, ci-après RGPD.

90 V. VERBRUGGEN, « Titre 1 - RGPD : coeur du puzzle de l'encadrement de la protection des données à caractère personnel dans l'Union Européenne », *Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Éditions Larcier, 2018, p. 27 ; Considérants n°9 et 10 du RGPD.

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

lorsque le droit belge décide d'exercer sa faculté lui permettant de diminuer à 13 ans l'âge plancher à partir duquel il est possible pour un mineur de donner son consentement au traitement de ses données à caractère personnel.[92]

Malgré ses fondements communs avec la directive, le RGPD comporte de nombreuses nouveautés.[93] Le champ d'application du règlement a été considérablement étendu,[94] les sanctions ont été alourdies,[95] les conditions entourant le consentement ont été bétonnées.[96] Le règlement met également en place une série de nouveaux droits subjectifs pour les personnes concernées par un traitement tels que le droit d'accès, le droit à l'effacement et le droit à la portabilité des données.[97] Enfin, il précise certains concepts tels que la protection des données dès la conception ou par défaut ,[98] et en crée d'autres comme celui de délégué à la protection des données.[99]

[92] Loi du 30 juillet 2018, *op. cit.*, article 5.
[93] A ce sujet voy. not. : https://eugdpr.org/the-regulation/, consulté le 12 avril 2019
[94] Article 3 du RGPD.
[95] Article 83 du RGPD, jusque 4% du chiffre d'affaires ou 20 millions d'euros, en fonction duquel est le plus grand.
[96] Article 7 du RGPD.
[97] Articles 15, 17 et 20 du RGPD.
[98] Article 25 du RGPD.
[99] Article 38 du RGPD.

Section 2. Les notions fondamentales du règlement

La matière de la protection des données à caractère personnel est ancrée au sein de l'Union Européenne. Il était nécessaire de mettre en place un cadre législatif clair et harmonisé entre les états membres afin de faciliter la mise en conformité des entreprises concernées. De plus, les notions employées sont totalement autonomes et méritent que nous nous y attardions.

Tout d'abord, nous étudierons successivement les concepts de "données à caractère personnel", de "traitement", de "responsable du traitement" et par là, le champ d'application matériel. Ensuite, nous traiterons succinctement du champ d'application territorial.

Sous-Section 1. Données à caractère personnel

La définition des données à caractère personnel est cruciale. En effet, c'est elle qui a pour objet de donner son étendue au champ d'application matériel du règlement. Elle doit être exhaustive pour prétendre à une protection efficace.

L'article 4.1 du règlement définit les données à caractère personnel comme : « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée"). Cette définition a été reprise mot pour mot de la directive.[100] Dès lors, les commentaires doctrinaux et prétoriens antérieurs à l'adoption du règlement restent pertinents.

À la lecture de cette définition, quiconque est en droit de s'étonner de son champ d'application très large. En réalité, c'est une volonté affirmée d'une part, par la Commission dès 1992 au sein des travaux préparatoires et d'autre part, par le Conseil, dans la position commune quant à la directive 95/46/CE.[101] Dans ces documents, ces institutions expliquent que « la proposition modifiée donne satisfaction à l'objectif du Parlement qui est d'adopter la définition la plus globale possible de la notion de "donnée à caractère personnel", afin de couvrir toutes [nous insistons] les informations qui peuvent être reliées à une personne physique. ».[102]

---

[100] Directive 95/46/CE, *op. cit.*, article 2, a).

[101] (CE) relative à l'adoption de la directive 95/46/CE en vue de l'adoption de la directive 95/46/CE du parlement et du conseil, du 24 octobre 1995, relative à la protection des données à caractère personnel et à la libre circulation de ces données*, J.O.C.E* 13 avril 1995*,* p. 20. ; Proposition amendée pour une directive du Conseil sur la protection des individus au regard du traitement de données personnelles et à la libre circulation de ces données, *COM(92) 422 final - SYN 287*, 28 octobre 1992, p. 9.

[102] Proposition amendée pour une directive du Conseil, *Ibid.*, p. 9.

§1 Les informations

N'importe quel type de donnée peut être considéré comme une donnée personnelle pour autant qu'elle satisfasse aux critères fixés par le RGPD. Il n'y a aucune restriction quant à la forme de celle-ci. Elle peut tant couvrir des situations privées que publiques. À cet égard, sa qualification de privée ou publique n'aura aucune incidence sur le niveau de protection octroyé par le règlement à cette donnée.[103]

Par exemple, dans le cadre du *quantified self*, le fait que des données soient accessibles à n'importe quel utilisateur d'une application ou uniquement à un cercle restreint n'aura aucune incidence sur la protection accordée à ces mêmes données.

De plus, le règlement concerne les données tant objectives que subjectives.[104] Dans le cadre du *quantified self*, cela se traduit non seulement par une protection des données relevées par l'application (objectives) mais également par la protection des conseils donnés afin d'améliorer le fruit de la quantification réalisée par l'utilisateur (subjectives).

Enfin, les données peuvent prendre des formes très diverses. Un écrit, un texte, un graphique, un dessin, des données biométriques ou encore génétiques sont éligibles à la protection offerte par le règlement.[105]

C'est donc une approche fidèle aux prémisses de cette règlementation qui a été reproduite dans le RGPD.

§2 Les personnes concernées

Afin que des données soient considérées comme personnelles, celles-ci doivent en plus d'être des données, comme expliqué ci-dessus, également concerner des personnes identifiées ou identifiables.[106]

---

[103] C.J.C.E., 16 décembre 2008, arrêt *Tietosuojavaltuutettu c. Satakunnan markkinapörssi oy et Satamedia o*y, C-73/07, pt 49.
[104] C. DE TERWANGNE, « Titre 2 - Définitions clés et champ d'application du RGPD », *op. cit.*, p. 62.
[105] *Ibid.*, p. 62
[106] Article 4.1 du RGPD.

A. Personne physique

Comme le mentionne le Groupe de l'article 29 dans un document de travail, la législation en la matière n'a pour objet de protéger que les personnes physiques dans le but de sauvegarder leurs droits fondamentaux.[107] C'est ce qui a été retranscrit au sein du considérant 14 du règlement. Celui-ci exclut expressément l'application de la législation aux personnes morales.[108]

Nous sommes conscients que se pose également la question des personnes décédées ou à naitre. Cependant, dans le cadre limité de ce propos, nous ne nous y attarderons pas.

B. Concernée

Afin qu'une donnée puisse être considérée comme personnelle, il doit y avoir un lien entre celle-ci et la personne physique. Dans de nombreux cas, il est aisé d'établir un lien direct entre la donnée et la personne. Par exemple, dans le cas d'un profil sur une application de sport, il est clair que ces données se rapportent au titulaire du profil.

Dans d'autres cas, la tâche peut se révéler plus complexe notamment lorsque les données se réfèrent à des choses et non à des personnes. Ce n'est donc que de manière indirecte que l'on pourra rattacher des données à des personnes. Par exemple, la valeur d'une maison ce n'est pas une donnée personnelle en soi mais cela renseigne sur le patrimoine de la personne concernée.[109]

Afin de pouvoir déterminer si une donnée concerne une personne physique ou non, il a été mis en place un système de trois critères alternatifs. Si une donnée en raison de son contenu, de sa finalité ou de son résultat, se rapporte à une personne physique, elle devra être considérée comme concernant cette personne.[110] Cette approche a été confirmée par la Cour de Justice dans son arrêt Novak de 2017.[111]

---

[107] Groupe de l'article 29, Avis 4/2007 sur le concept de données à caractère personnel, WP 136, 20 juin 2007, p. 4, disponible en ligne à l'adresse : « https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf », consulté le 12 avril 2019.
[108] Considérant n°14 du RGPD.
[109] Groupe de l'article 29, Avis 4/2007, *op. cit.,*p. 10.
[110] Groupe de l'article 29, *Ibid.,* p. 11.
[111] C.J.U.E., 20 décembre 2017, arrêt *Novak*, C-434/16, pt 35.

C. Identifiée ou identifiable

Enfin, après s'être rapportée à une personne physique, la donnée en question doit également permettre d'identifier une personne de manière directe ou indirecte.[112]

L'identification revêt ici une portée spécifique. Elle ne doit pas être comprise comme le fait de pouvoir mettre un nom et un prénom sur un profil. En effet, il n'est souvent pas nécessaire de détenir ces informations pour que l'on puisse isoler une personne. La question est plus de savoir s'il est possible d'individualiser une personne plutôt que de pouvoir dire qui elle est avec précision.[113]

Afin de définir si une personne est identifiable au sens du règlement, le considérant 26 nous donne les précisions suivantes : « Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tel que le ciblage. »

En d'autres termes, il faut apprécier si la mise en oeuvre de moyens raisonnables, tant au niveau technologique que financier, permet de remonter vers un profil individualisable. Si les données en question ne permettent pas de remonter vers un tel profil, elles seront considérées comme anonymes. Par conséquent, elles échapperont à la qualification de données à caractère personnel et seront exclues du champ d'application du règlement.

Cependant, se reposer sur des techniques d'anonymisation afin d'échapper à l'application du règlement est risqué. Pour déterminer si une donnée est anonyme, il convient de se référer au considérant 26 du RGPD, qui comme précité, énonce que le critère principal pour identifier une personne est « l'ensemble des moyens raisonnablement susceptibles d'être utilisés ».[114] Ce critère doit être sans cesse réévalué au regard de l'évolution de la technologie. Ainsi, une donnée, autrefois anonyme, peut désormais se retrouver soumise au règlement. Par exemple, il y a plusieurs années,

---

[112] Article 4.1 du RGPD.

[113] Groupe de l'article 29, Avis 4/2007, *op. cit.,* pp. 13 et s. ; C. DE TERWANGNE, « Titre 2 - Définitions clés et champ d'application du RGPD », *op. cit.*, p. 64. ; A. CASSART, A. CATTEAU, F. COTON, S. DELCOMINETTE, F. ERNOTTE, N. HAMBLENNE, P. LIMBRÉE,V. RONNEAU et A. VAN DEN BRANDEN, *Le droit des Machintechs (FinTech, Legal Tech, MecdTech,…), État des lieux et perspectives*, Bruxelles, Larcier, Coll. Jeune Barreau du Brabant Wallon, 2018.

[114] Considérant n°26 du RGPD.

une donnée pouvait être considérée comme anonyme car il était hors de prix de remonter jusqu'à un certain profil pour l'individualiser alors que ce coût est, aujourd'hui, plus abordable.[115]

§3 Les données sensibles

Les données sensibles sont une catégorie de données à part qui méritent une attention particulière de la part du règlement. Celui-ci les classe en deux catégories distinctes. La première catégorie est générale et comprend notamment les données biométriques, génétiques et de santé. Elles sont traitées au sein de l'article 9 qui leur prévoit un régime particulier. La seconde catégorie concerne les données relatives aux condamnation pénales. Elles sont régies par l'article 10 qui leur prévoit, lui aussi un régime particulier.

Dans le cadre de ce propos, nous traiterons uniquement du régime applicables aux données sensibles générales. En effet, les données biométriques, génétiques et de santé, étant au coeur des outils du *quantified self*, elles revêtent une importance capitale au sein se ce propos.

Afin de déterminer quelle est la qualification la plus adéquate à attribuer aux données sensibles récoltées par les outils de *quantified self* tels que les battements du coeur, l'activité physique, les performances physiques,… il convient de distinguer les trois notions de génétique, biométrique et de santé.

Tout d'abord, les données génétiques sont relatives à des caractéristiques génétiques héréditaires, qui donnent des informations sur la biologie et qui résultent notamment d'une analyse d'un échantillon biologique.[116] Nous pouvons raisonnablement affirmer que ce type de données ne concerne pas les outils de *quantified self*.

Ensuite, les données biométriques, sont : « les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques ».[117] Ce sont donc des données qui

---

[115] Groupe de l'article 29, *Opinion 05/2014 on anonymisation techniques,* 10 avril 2014, WP216 ; C. DE TERWANGNE, « Titre 2 - Définitions clés et champ d'application du RGPD », *op. cit.*, p. 64. ; A. CASSART, A. CATTEAU, F. COTON, S. DELCOMINETTE, F. ERNOTTE, N. HAMBLENNE, P. LIMBRÉE,V. RONNEAU et A. VAN DEN BRANDEN, *op. cit.*

[116] Article 4.13 du RGPD

[117] Article 4.14 du RGPD

doivent confirmer l'identité de la personne.[118] Ce type de données n'est pas récolté par les outils de *quantified self* tels qu'analysés ici.

Enfin les données de santé, sont : « relatives à la santé physique ou mentale d'une personne physique,[…], qui révèlent des informations sur l'état de santé de cette personne ».[119] La fin de la définition est importante car elle exprime que la révélation même la plus infime sur un état de santé suffit pour qualifier la donnée comme sensible et pour que le régime subséquent s'applique.[120]

C'est une définition qui ne manque pas de susciter de nombreuses interrogations notamment concernant son application. L'affaire la plus connue concernant l'application de cette notion est l'arrêt *Lindqvist.* Dans cette affaire, Mme Lindqvist responsable d'une paroisse et de son site internet, a mis en ligne des données concernant la blessure au pied d'une de ses collègue et par conséquent, de son arrêt de travail. La Cour a considéré que les actes de Mme Lindqvist constituaient un traitement de données sensibles. Elle précise qu'un tel traitement, doit respecter les principes de la Directive (aujourd'hui le RGPD). Or, celle-ci implique une interdiction de traitement des données sensibles.[121] À travers cet exemple, on remarque la portée de cette définition que l'on pourra qualifier dans certains cas d'excessive.[122]

Cette définition sur les données de santé concerne particulièrement les outils du *quantified self*. En effet, de nombreuses données telles que l'activité quotidienne, le nombre de pas, les performances physiques, le rythme cardiaque,… sont des données qui révèlent des informations sur la santé. Par conséquent, s'appliquera le régime de traitement particulier prévu par l'article 9.[123]

---

[118] ; Considérant 51 du RGPD ; J.-M. VAN GYSEGHEM, « Les catégories particulières de données à caractère personnel », *Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Éditions Larcier, 2018, p. 262.

[119] Article 4.15 du RGPD.

[120] J.-M. VAN GYSEGHEM, « Les catégories particulières de données à caractère personnel », *op. cit.*, p. 263.

[121] C.J.C.E., 6 novembre 2003, arrêt *Lindqvist*, C-101/01.

[122] J.-M. VAN GYSEGHEM, « Les catégories particulières de données à caractère personnel », *op. cit.*, p. 265.

[123] Voy. *infra*, Sous-Section 2. Traitement, §5 Traitement de données sensibles.

Sous-Section 2. Traitement

§1 Notion

La notion de traitement est également essentielle au sein de cette matière. Elle est définie directement au sein de l'article 4.2 du RGPD qui indique de manière exhaustive l'ensemble des opérations techniques qualifiées de traitement.[124]

L'objectif de protection est resté identique par rapport aux travaux précédant l'adoption de la directive : une définition extensive qui aura pour but d'inclure toutes les opérations susceptibles d'être effectuées sur des données. En effet, selon les rédacteurs, une définition extensive est le meilleur moyen d'assurer une protection effective des individus car elle couvre toute opération de la collecte à l'effacement des données.[125]

Dès lors, toute manipulation de données devra être qualifiée de traitement et, pour autant que les autres conditions soient remplies, emportera application du règlement.

§2 Principe de loyauté et de transparence

Une des obligations présentes dans le RGPD est que le traitement des données soit réalisé de manière loyale.[126] Il s'agit, en quelque sorte, d'une obligation de bonne foi imposée au responsable du traitement envers la personne concernée. Il doit donc annoncer l'objectif dans lequel les données récoltées vont être traitées.[127] Le considérant 60 du RGPD précise d'ailleurs que ce principe exige que la personne concernée soit informée de l'existence de l'opération de traitement et de ses finalités.

En ce qui concerne le principe de transparence, le considérant 39 du règlement exprime que les informations concernant le traitement de données devrait être explicitées de manière claire au sein de la politique de vie privée de façon à ce que chacun puisse comprendre ce qu'il adviendra de ses

---

[124] «traitement», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;

[125] Proposition amendée pour une directive du Conseil, *op. cit.*, p. 9.

[126] Article 5.1.a du RGPD.

[127] DE TERWANGNE, C., « Titre 3 - Les principes relatifs au traitement de données à caractère personnel », *op. cit.* pp. 90 et 91.

données. Cela concerne également les droits, les risques, les règles et les garanties liés à ce traitement de données.

On remarque au sein de ce considérant 39, l'utilisation du conditionnel présent comme temps de conjugaison. Selon nous, ce choix exprime certainement l'idée de voir ces principes plus comme un objectif idéal à atteindre, une marche à suivre plutôt qu'une obligation à proprement parler. Comme nous le détaillerons plus loin dans l'analyse des pratiques de traitement de données dans le cadre du *quantified self*, il n'y a que très peu de personnes qui lisent les politiques de confidentialité. Ce qui a notamment pour conséquence que la transparence s'en voit affaiblie.[128]

§3 Finalité déterminée et explicite

Afin que la personne concernée puisse se rendre compte de ce qui va être fait de ses données, le responsable du traitement doit définir au sein de sa politique de confidentialité, les utilisations prévues pour les données récoltées.[129] Cette finalité doit respecter plusieurs critères : elle doit être déterminée, explicite et légitime.[130]

Le concept de "déterminé" exprime l'idée que la description doit être assez précise pour que la personne concernée puisse déterminer ce que vont subir ses données en délimitant les opérations à venir et pour que, le cas échéant, elle puisse exercer ses droits.[131]

La définition des usages doit, en outre, être "explicite". c'est à dire qu'elle doit être aisément accessible pour les personnes concernées qui souhaiteraient les consulter.[132]

Enfin, elle doit être "légitime". Cela va plus loin que la simple légalité du traitement, nous sommes ici dans une notion à géométrie variable qui s'apprécie selon le cas d'espèce. On notera par contre que la contrariété à la loi présume d'office l'absence de légitimité.[133] C'est dès lors une question de mise en balance : la finalité pour laquelle ces données sont traitées et les intérêts du responsable du

---

[128] A. VIEL, S. KINGSMILL, J. MACLEOD, *Privacy for sale – To the highest bidder,* Deloitte report, 2017, disponible à l'adresse : « https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/deloitte-analytics/ca-en-data-ethics-and-privacy-survey.pdf », consulté le 16 avril 2019.

[129] Article 5.1.b du RGPD.

[130] DE TERWANGNE, C., « Titre 3 - Les principes relatifs au traitement de données à caractère personnel », *op. cit.,* pp. 94 à 96.

[131] Groupe de l'article 29, Opinion 03/2013 on purpose limitation, 2 avril 2013, p.12, disponible en ligne à l'adresse : « https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp203_en.pdf », consulté le 16 avril 2019.

[132] *Ibid.*

[133] *Ibid.*

traitement ne peuvent porter atteinte de façon disproportionnée aux droits de la personne concernée.[134]

§4 Principe de licéité du traitement

Dans le cadre de la protection des données à caractère personnel, il est nécessaire que les données soient traitées de façon licite. Il doit y avoir une base légale sur laquelle les données sont traitées. Nous analyserons les deux bases les plus pertinentes pour rendre licite un traitement de données dans le cadre d'outils de *quantified self*.[135] Tout d'abord, nous nous attarderons sur le consentement, qui n'est pas sans poser de lourdes questions éthiques et ensuite, nous traiterons du contrat, qui permet à un responsable du traitement de traiter les données personnelles nécessaires à l'exécution d'un contrat pour autant qu'elles ne soient pas sensibles.

A. Le consentement

Le consentement est une des six méthodes sur lesquelles peut se reposer un responsable du traitement pour justifier le traitement qu'il opère.[136] C'est une notion qui suscite beaucoup de discussions. Alors que certains considèrent qu'il est l'élément clé permettant de légitimer un traitement de données afin que la personne concernée puisse contrôler ses données,[137] d'autres estiment que la notion de consentement doit être plus nuancée en fonction des situations.[138]

---

[134] DE TERWANGNE, C., « Titre 3 - Les principes relatifs au traitement de données à caractère personnel », *op. cit.,* pp. 94 à 96.

[135] Nous sommes conscients qu'il existe également quatre autres bases susceptibles de légitimer un traitement de données, à savoir : le respect d'une obligation légale (article 6.1.c. du RGPD), la sauvegarde des intérêts vitaux de la personne concernée (Article 6.1.d. du RGPD), l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique (article 6.1.e du RGPD) et enfin des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée (article 6.1.f du RGPD). Nous le traiterons pas eu égard à leur pertinence limitée quant au sujet abordé.

[136] Article 6.1.a du RGPD.

[137] Comité LIBE du Parlement Européen, Rapport sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), 21 novembre 2013, pp. 218 et 219.

[138] C. LAZARO et D. LE METAYER, « Consent to Personal Data Processing: A Comparative Perspective on Data Subject's Autonomy », *R.J.T.,* 2014, pp. 800 et s., disponible en ligne à l'adresse : « http://heinonline.org/HOL/Index?index=journals/revjurns&collection=journals », consulté le 16 avril 2019.

i. Notion

- *Définition*

La matière du consentement est réglée par l'article 6.1.a du RGPD qui trouve appui sur les considérants 32, 33, 42, 43 et 44. Il est défini par le règlement comme : « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».[139]

- *Par une déclaration ou un acte positif clair*

Alors que la majorité de la définition reste identique à celle contenue dans la directive, elle a reçu un renforcement depuis le règlement.[140] En effet, des ajouts concernant la façon dont le consentement peut être donné ont été insérés. Ce changement intervient pour préciser la notion de « toute manifestation de la volonté ».

Auparavant, les termes "par une déclaration ou un acte positif clair" n'existaient pas, cela donnait donc lieu à des situations où le consentement pouvait être reçu de manière tacite.[141] De plus, de par l'instrument choisi afin de légiférer, les interprétations nationales se révélaient divergentes sur le fait d'accepter ou non le consentement tacite.[142] Cette controverse est désormais abolie par l'introduction des termes : "par une déclaration ou par un acte positif clair". Le règlement précise en outre que le consentement ne peut résulter du silence ou d'une inactivité.[143]

---

[139] Article 4.11 du RGPD.

[140] E. POLITOU, E. ALEPIS et C. PATSAKIS, « Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions », *Journal of cyber security*, 2018, Department of Informatics, University of Piraeus, Piraeus, p. 6, disponible en ligne à l'adresse : « https://tinyurl.com/Forgettingpersonaldata », consulté le 21 avril 2019.

[141] Groupe de l'article 29, Avis 15/2011 sur la définition du consentement, WP 187, 13 juillet 2011, p. 12, disponible en ligne à l'adresse : « https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp187_fr.pdf », consulté le 16 avril 2019.

[142] *Ibid.*, p. 6.

[143] Considérant 32 du RGPD.

ii. Qualités du consentement

L'article 4.11 désigne une liste de qualités que doit rencontrer le consentement afin de pouvoir rendre un traitement licite.

- *Libre*

Tout d'abord, il doit être libre. Afin de déterminer si celui-ci peut être libre, il est nécessaire d'avoir égard à plusieurs situations. Premièrement, lorsqu'il existe un rapport de force disproportionné entre les parties, il faudra considérer que le consentement ne peut être considéré comme libre. Dès lors dans le cadre d'un contrat de travail ou d'une relation avec une autorité publique, il faudra se baser sur d'autres moyens afin de rendre licite le traitement.[144]

Deuxièmement, une autre manière de s'assurer du caractère libre du consentement est de vérifier que celui-ci ne porte que sur le traitement des données à caractère personnel. En effet, il ne peut pas être lié au contrat. En pratique, cela signifie que d'une part, il n'est plus possible d'insérer une partie sur le traitement au sein des conditions générales d'utilisation. D'autre part, la politique de vie privée doit être distincte. À défaut, le règlement considèrera que le consentement ne peut avoir été donné librement.[145]

Troisièmement, afin d'être qualifié de libre, il doit également se conformer à l'absence de préjudice en cas de retrait. C'est-à-dire que dans le cas où une personne concernée décide ne plus donner son consentement pour toutes les finalités de traitement, elle ne peut subir en retour aucune conséquence négative.[146] Par exemple, un utilisateur d'une application de *quantified self* qui consent au traitement de ses données à des fins publicitaires qui désire ensuite revenir sur son choix ne peut pas voir les fonctionnalités de son application limitées.

---

[144] Groupe de l'article 29, Lignes directrices sur le consentement au sens du règlement 2016/679,WP 269 rév.1 ,10 avril 2018, pp. 6 à 8, disponible en ligne à l'adresse : « https://www.cnil.fr/sites/default/files/atoms/files/ldconsentement_wp259_rev_0.1_fr.pdf », consulté le 16 avril 2019 ; C. DE TERWANGNE, « Titre 3 - Les principes relatifs au traitement de données à caractère personnel », *op. cit.,* p. 121 ; Considérants 42 et 43 du RGPD.

[145] Considérant 43 du RGPD ; Groupe de l'article 29, Lignes directrices sur le consentement au sens du règlement 2016/679, *op. cit.,* p.9 ; Considérant 43 du RGPD ; Information Commissioner's Office, *Consultation: GDPR consent guidance*, 30 mars 2017, p. 19, disponible en ligne à l'adresse : « https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf », consulté le 17 avril 2019.

[146] Groupe de l'article 29, Lignes directrices sur le consentement au sens du règlement 2016/679, *op. cit.,* p. 11 ; Considérant 42 du RGPD.

• *Spécifique*

Ensuite, le consentement doit être spécifique. Cela signifie que lorsque le traitement est opéré à différentes fins, les personnes concernées doivent avoir le droit de donner ou non leur consentement pour chacune de ces finalités. Il se peut dès lors que le consentement soit multiple, c'est ce qu'on appelle alors la "granularité". L'absence de spécificité présume également de la non liberté du consentement.[147] Par exemple, un utilisateur pourra consentir au traitement de ses données sensibles telles que son rythme cardiaque pour une analyse de ses performances physiques et ne pas consentir au traitement de ces mêmes données à des fins publicitaires.

Malgré l'objectif d'harmonisation présent au sein du règlement, la notion de "granularité" a déjà fait l'objet d'interprétation différenciées par les Cours Suprêmes de deux états membres : l'Autriche et l'Italie. Alors que la Cour Autrichienne a considéré que la granularité du consentement devait être absolue,[148] la Cour Italienne a, quant à elle, décidé que cette notion pouvait être appréciée à l'aune d'une mise en balance des intérêts des parties en question.[149] Dans cette matière, les deux cours ont usé de la doctrine selon laquelle il n'est pas nécessaire de poser une question préjudicielle lorsque la loi est claire.

Certains interprètent cette divergence de jugement entre les deux Cours par la différence dans les termes utilisés au sein des versions allemande et italienne du RGPD. Dans la version germanique, le consentement est "réputé" ne pas avoir été donné librement en cas de non-granularité,[150] alors que, dans la version italienne le mot "présumé" est utilisé.[151]

La Cour de Justice de l'Union devra donc, malgré le choix d'un règlement comme outil législatif, se confronter à des interprétations législatives divergentes et, par conséquent, y mettre de l'ordre.

---

[147] Groupe de l'article 29, Lignes directrices sur le consentement au sens du règlement 2016/679, *op. cit.,* p. 11 ; Considérants 32 et 43 du règlement.

[148] Cour Suprême autrichienne, 30 aout 2018, 6 Ob 140/18h, disponible en ligne à l'adresse : « https://www.lexfutura.ch/fileadmin/lexfutura.ch/Bilder/Blog/OGH_31.08.2018_6_Ob_140_18h.pdf », consulté le 19 avril 2019.

[149] Cour suprême de Cassation italienne, 2 juillet 2018, n°17278/2018, disponible en ligne à l'adresse : « https://www.lexfutura.ch/fileadmin/lexfutura.ch/Bilder/Blog/_20180702_snciv%40s10%40a2018%40n17278%40tS.clean.pdf », consulté le 19 avril 2019.

[150] Considérant 43 du RGPD, version allemande : « Die Einwilligung gilt nicht als freiwillig erteilt », traduction libre.

[151] *Ibid*., version italienne : « Si presume che il consenso non sia stato liberamente espresso », traduction libre.

- *Éclairé*

Le consentement est défini comme "éclairé", ce qui diffère de l'ancienne version qui utilisait le terme "informé". Selon C. DE TERWANGNE, ce changement ne doit pas apporter de nouvelle signification quant à sa portée.[152] Afin de pouvoir rencontrer cette qualité il faut qu'un certain nombre d'informations soit communiqué à la personne concernée. Le caractère éclairé est donc étroitement lié aux principes de loyauté et de transparence. Selon le groupe de l'article 29, il est nécessaire qu'au minimum 6 exigences soient rencontrées afin de pouvoir considérer le consentement comme éclairé, à savoir : l'identité du responsable du traitement, les finalités, le type de données collectées, le droit de retrait, les informations concernant la prise de décision automatisée ainsi que les divers risques liés au traitement.[153]

En ce qui concerne la formulation des informations, le RGPD tâche d'améliorer l'intelligibilité et la compréhension aisée des informations.[154] Il faut vraiment que le consentement soit donné sur base d'une formulation simple qui permette aisément de comprendre ce à quoi l'on s'engage.

- *Univoque*

Enfin, le consentement se doit d'être univoque, ce qui rejoint la notion de « déclaration ou d'acte positif clair » introduit au début de ce point. Cela exprime notamment l'idée que le consentement donné doit être indubitable, ce qui peut mais ne doit logiquement pas résulter d'une simple lecture de le politique de confidentialité mais bien d'une compréhension claire de ce qui sera fait des données.[155] Le considérant 32 explique notamment qu'une case pré-cochée n'est pas à même de satisfaire cette condition. L'approche de ce considérant est quelque peu étonnante par rapport à l'économie globale du règlement. Alors que l'ensemble de cette nouvelle législation plaide pour un renforcement de la conscience de la personne concernée face au traitement de données, il est ici expressément admis que le simple fait de cocher une case peut fonder un moyen de recueillir un consentement aussi complexe que celui présenté ci-dessus… Selon le groupe de l'article 29, la meilleure façon de faire est de recueillir une déclaration écrite de la part de la personne concernée

---

[152] DE TERWANGNE, C., « Titre 3 - Les principes relatifs au traitement de données à caractère personnel », *Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Éditions Larcier, 2018, p. 128.
[153] Groupe de l'article 29, Lignes directrices sur le consentement au sens du règlement 2016/679, *op. cit.,* p.15.
[154] Article 7.2 et considérant 32 du RGPD
[155] Information Commissioner's Office, *Consultation: GDPR consent guidance*, *op. cit.*, p.22.

dans laquelle elle détaillerait ce à quoi elle consent. Il réalise tout de même que cette hypothèse est très peu plausible.[156]

Il est à noter qu'en vertu du principe d' "*accountability*" le responsable du traitement, celui-ci devra être en mesure de prouver la réunion de ces éléments.[157]

iii. Retrait du consentement

En plus de ces conditions concernant les qualités même du consentement, le RGPD met en place un droit au retrait du consentement permettant d'en garantir l'intégrité.[158] Il prend notamment place dans les notions de liberté et de spécificité du consentement. Il est subordonné aux mêmes conditions que lorsque la personne concernée donne son consentement.[159] En conformité avec la notion de granularité, le consentement peut donc être retiré pour tout ou partie des finalités. Ce retrait n'affecte, par contre, pas la légalité du traitement opéré lorsque le consentement était utilisé comme base légale.[160]

De plus lorsque le traitement des données ne se justifie plus sur aucune des six bases, naît dans le chef de la personne concernée un droit à l'effacement des données.[161] Ce qui a pour conséquence directe de soumettre à un aléa relativement élevé la légalité du traitement effectué par le responsable du traitement qui, du jour au lendemain, pourrait se retrouver sans aucune base légale pour le traitement de certaines données à caractère personnel et pourrait également se voir contraint de les effacer.[162]

Selon Monsieur BAIJOT, c'est une notion qui ne pose que peu de problèmes en pratique. En effet, les données de chacun étant regroupées, il est facile d'identifier ce qu'il est nécessaire de supprimer comme données. Il n'ont eu que très peu de demandes à ce sujet.[163]

---

156 Groupe de l'article 29, Lignes directrices sur le consentement au sens du règlement 2016/679, *op. cit.,* p.18.
157 Article 7.1 et considérant 42 du RGPD ; Pour le principe d' *« accountabilty* », voy. *infra* : Sous-Section 3, Paragraphe 3.
158 Article 7.3 du RGPD.
159 Considérant 42 du RGPD ; European Data Protection Supervisor, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 14 mars 2017, p. 18.
160 Article 7.3 du RGPD.
161 Article 17 du RGPD.
162 C. DE TERWANGNE, « Titre 3 - Les principes relatifs au traitement de données à caractère personnel », *op. cit.,* p. 128.
163 Interview L. BAIJOT, Annexe, Question 4.

B. Le contrat

Le règlement prévoit plusieurs méthodes afin de légaliser le traitement des données, le contrat est la deuxième. Le traitement devient légal s'il « est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures pré-contractuelles prises à la demande de celle-ci ».[164]

Le contrat a pour avantage d'être basé sur des critères objectifs et non subjectifs, ce qui le rend plus sûr et bien plus légitime qu'un consentement médiocre. Afin qu'il puisse exercer ses effets, deux conditions doivent être remplies : la participation au contrat de la personne concernée et la nécessité de traitement en vertu du ce contrat.[165]

Il faut donc en premier lieu que ce soit la personne concernée partie au contrat qui soit impliquée c'est-à-dire que si une partie du traitement concerne d'autres personnes, cette partie devra être soumise à une autre base légale permettant de la légitimer. Cela nous renvoie dès lors à la granularité du consentement.

Ensuite, le traitement doit être nécessaire à l'exécution du contrat. La notion de nécessité est particulièrement difficile à appréhender. Elle relève d'une appréciation au cas par cas en fonction du cas d'espèce, c'est-à-dire en fonction de la finalité de traitement pour laquelle la légalisation par contrat est nécessaire. De plus, elle ne doit pas être appréciée de façon restrictive, elle ne doit concerner que l'exécution du contrat.[166] Cette dernière condition peut être particulièrement difficile à appréhender car ce sont directement les prestataires de services qui définissent cette notion.

Une remarque doit cependant être faite concernant la matière du *quantified self*. En effet, les données collectées dans ce cadre se révèleront en partie être des données sensibles. Comme nous le verrons dans le paragraphe suivant, le traitement de données sensibles ne peut devenir licite sur la base de l'exécution d'un contrat. Les hypothèses sont différentes de celles concernant les données « ordinaires ». Dès lors, les seules données qui pourront être traitées sur cette base seront assez restreintes. On peut par exemple citer les informations de base lors de l'inscription : nom, prénom,

---

164 Article 6.1.b du RGPD.

165 Groupe de l'article 29, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE , WP 217, 9 avril 2014, disponible en ligne à l'adresse : «https://www.alain-bensoussan.com/wp-content/uploads/2016/09/20140409.pdf », consulté le 17 avril 2019.

166 Groupe de l'article 29, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE , *op. cit.*, p. 18.

adresse, e-mail,… Par contre, pour ce qui est du poids, de la fréquence des entraînements, de la qualité du sommeil, de l'alimentation,… il ne sera pas possible de prendre appui sur le contrat afin de légaliser le traitement, eu égard à leur caractère sensible.

§5 Traitement de données sensibles

Les données sensibles sont une catégorie de données à part. Dans le cadre de ce propos, nous concentrerons notre propos sur le cas des données de santé, car ce sont les données les plus pertinentes dans le contexte du *quantified self*.[167]

Comme nous l'avons vu précédemment dans ce propos, une régime particulier est applicable au consentement de telles données, l'article 9 du RGPD procède à une inversion de paradigme. En effet, alors que les données ordinaires peuvent être traitées mais uniquement sur la base d'un des moyens limitativement énoncés par le règlement, les données sensibles souffrent d'une interdiction générale de traitement.[168]

Malgré cette interdiction, le règlement prévoit plusieurs hypothèses dans lesquelles il pourra tout de même être procédé au traitement des données de santé. Dans le cadre limité de ce propos, nous ne nous attarderons que sur l'hypothèse du consentement explicite au traitement des données.[169] Celui-ci est une version renforcée du consentement nécessaire pour le traitement des données ordinaires. De plus, les autres hypothèses ne nous intéressent que peu dans le cadre du *quantified self*.[170]

Le consentement explicite ne vise pas à s'appliquer uniquement en matière de légalisation du traitement des données sensibles, il trouve aussi sa place dans le cadre du transfert vers des pays tiers ainsi que dans le cadre du profilage.[171]

L'ajout du terme "explicite" implique donc un renforcement du consentement par rapport aux traitement des données ordinaires. Conformément au considérant 43 du règlement, lorsqu'un

---

[167] Pour une définition des données sensibles, voy. *supra* : Sous-Section 1 Données à caractère personnel, §3 Données sensibles.
[168] Articles 5, 6 et 9 du RGPD.
[169] Article 9.2.a du RGPD.
[170] Articles 9.2.b à 9.2.j du RGPD.
[171] Articles 49 et 22 du RGPD.

consentement explicite est exigé, il est nécessaire que celui-ci soit donné séparément de celui donné pour la ou les autre(s) finalité(s) prévues par le responsable du traitement.[172]

Idéalement, le consentement explicite devrait faire l'objet d'une déclaration écrite de la personne concernée dans laquelle elle indiquerait qu'elle autorise le traitement des données pour des finalités définies. Malheureusement, les outils numériques ne permettent que rarement d'obtenir cette déclaration.[173]

Sous-Section 3. Responsable du traitement et sous-traitant

Les notions de "responsable du traitement" et de "sous-traitant" sont également essentielles. En effet, la désignation d'un ou plusieurs responsables de traitement détermine le débiteur des obligations mises en place par le règlement. Ces obligations varient en fonction de l'implication de la personne qui traite les données. Nous étudierons succinctement les critères permettant d'attribuer la qualité de responsable du traitement ou de sous-traitant. Il est nécessaire de souligner que, dans leurs définitions, ces notions sont identiques à celles de la directive, les documents antérieurs au règlement restent donc pertinents à cet égard.[174]

§1 Le responsable du traitement

L'article 4.7 du RGPD[175] fixe trois critères cumulatifs permettant définir le responsable du traitement. Ils sont essentiels lorsque l'on recherche une quelconque responsabilité dans cette matière.

En premier lieu, il faut que ce soit : « Une personne physique ou morale, une autorité publique, un service ou un autre organisme ». Les termes "ou un autre organisme" attestent encore une fois de la

---

[172] Information Commissioner's Office, *Consultation: GDPR consent guidance*, 30 mars 2017, p.24, disponible en ligne à l'adresse : « https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf », consulté le 17 avril 2019.

[173] Groupe de l'article 29, Lignes directrices sur le consentement au sens du règlement 2016/679, *op. cit.,* p.22.

[174] A. DELFORGE, « Les obligations générales du responsable du traitement et la place du sous-traitant », *Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Éditions Larcier, 2018, p. 372 ; Articles 4.7 et 4.8 du RGPD ; Articles 2.d et 2.e de la Directive.

[175] «responsable du traitement», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre;

volonté d'un champ d'application extrêmement large afin de pouvoir inclure tous les potentiels sujets.[176]

Dans un deuxième temps, les termes suivants sont utilisés : "seul ou conjointement". Eu égard à l'évolution des technologies et à une tendance à la division des tâches, plusieurs sujets peuvent se voir attribuer la notion de responsable du traitement car plusieurs entités peuvent être amenées à traiter des données conjointement.[177] C'était une volonté claire de la Commission, lorsqu'elle a rendu son avis de directive amendée, que de permettre d'avoir plusieurs responsables conjoints pour un seul traitement de données.[178]

Dès lors, lorsque deux sujets sont amenés à traiter des données dans la même finalité avec des moyens propres ou identiques, ils pourront tous deux être considérés comme responsables du traitement. Le risque était cependant de voir les deux responsables du traitement se rejeter la faute en cas de réclamation d'une personne concernée. Le RGPD[179] a choisi d'immédiatement tarir cette potentielle source de conflit en permettant à la personne concernée d'exercer ses droits auprès du responsable du traitement de son choix.[180]

Enfin, pour être qualifié de responsable du traitement, il faut que le sujet en question détermine les moyens et les finalités du traitement. L'issue de cette question est généralement laissée à des considérations de fait. Il faut identifier qui, dans les faits, prend les décisions quant au traitement des données. Par exemple, le contrat sera un outil de choix afin d'appréhender qui peut être considéré comme responsable du traitement, surtout s'il reflète adéquatement les faits. De plus, il faudra apprécier l'ensemble de l'économie de ce contrat, une simple désignation non suivie dans la réalité sera insuffisante.[181]

Le responsable du traitement est donc le sujet capable de désigner les finalités du traitement, autrement dit le pourquoi, et les moyens utilisés pour les atteindre, c'est-à-dire le comment. À cet

---

[176] GROUPE 29, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », WP 169, p. 16, disponible en ligne à l'adresse : « http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf », consulté le 20 mars 2019.

[177] *Ibid*., p.19.

[178] Proposition amendée pour une directive du Conseil sur la protection des individus au regard du traitement de données personnelles et à la libre circulation de ces données *op. cit.*

[179] Article 26, §3 du RGPD.

[180] A. DELFORGE, « Les obligations générales du responsable du traitement et la place du sous-traitant », *op. cit.,* p. 376.

[181] *Ibid.* ; GROUPE 29, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », op. *cit.*, p. 16.

égard, il n'est pas nécessaire que le responsable du traitement désigne tous les moyens et finalités, une influence déterminante s'avère suffisante.

§2 Le sous-traitant

Le sous-traitant est quant à lui un exécutant du responsable du traitement. La principale différence entre ces deux notions réside dans le pouvoir de déterminer ou non les finalités et les moyens du traitement. Cela se remarque notamment au sein de la définition du sous-traitant contenue dans le RGPD qui reprend la même formulation que pour le responsable du traitement en ce qui concerne la forme juridique du sujet titulaire de cette qualité.[182]

Afin de recevoir la qualité de sous-traitant, il faut "agir pour le compte d'un tiers".[183] Ce qui signifie que le sous-traitant devra simplement exécuter ce qu'on lui a demandé. Il exécute donc un traitement de données mais sans jamais avoir d'influence sur ce qui lui est demandé de faire.[184] À défaut, il devra également être qualifié de responsable du traitement. Le seul cas où un sous-traitant peut s'éloigner de manière significative de ce qui a été fixé pour le traitement par le responsable, c'est lorsque le traitement violerait des obligations légales.

La qualification de responsable du traitement ou de sous-traitant est cruciale pour les sujets concernés car les obligations attachées à la notion de responsable du traitement sont bien plus élevées que celles du sous-traitant.

§3 Principe d'« accountability »

Ce principe dénommé en anglais "*accountability*",[185] ou en français de "responsabilité" désigne l'obligation générale pour les responsables de traitement de pouvoir démontrer la légalité de toutes leurs activités de traitement de données.[186] Il est une sorte de révolution en la matière car il fait désormais peser une obligation juridique de résultat sur les responsables du traitement.

---

[182] Article 4.8 du RGPD.
[183] *Ibid.*
[184] GROUPE 29, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », *op. cit.*, p. 27.
[185] Article 24 du RGPD.
[186] European Data Protection Supervisor, « Accountability », disponible en ligne à l'adresse : « https://edps.europa.eu/data-protection/our-work/subjects/accountability_en »,consulté le 17 avril 2019.

Par exemple, lorsqu'ils désirent s'appuyer sur cette notion, les responsables doivent être capables de démontrer les mesures techniques mises en place afin de pouvoir recueillir un consentement qualifié d'explicite lors de la collecte de données qualifiées de sensibles. De plus, ce principe les oblige a s'assurer que toutes les politiques de vie privée soient effectivement acceptées.[187]

Dès lors, l'ensemble des obligations incombant aux responsables du traitement présenté ci-dessus pourra faire l'objet d'une demande afin qu'il en soit démontré l'effectivité. Ce principe pousse alors les débiteurs de cette obligation à mettre en oeuvre le principe de "protection des données dès la conception", c'est-à-dire des systèmes qui sont à l'origine respectueux de la vie privée, ainsi que celui de "protection des données par défaut", c'est-à-dire qu'en l'absence de choix de la part de la personne concernée, la vie privée sera respectée.[188]

Sous-Section 4. Champ d'application territorial

Véritable révolution par rapport à la Directive, la champ d'application territorial de cette législation a reçu une extension considérable dans le RGPD. Confronté à de nombreuses entreprise étrangères à l'Union Européenne, il aurait été trop injuste que des personnes soient privées de leur droits à cause du lieu d'établissement hors Union du responsable du traitement.[189] Un système de trois critères alternatifs qui conditionnent l'application spatiale du RGPD a donc été mis en place. Nous étudierons successivement ces critères..

§1 Établissement d'un responsable du traitement ou sous-traitant au sein de l'Union Européenne

Tout d'abord, le critère le plus probable pour l'application du règlement est celui de l'établissement du responsable du traitement ou du sous-traitant au sein de l'Union Européenne.[190] La notion d'établissement n'est pas définie dans les articles du règlement. Cependant, le considérant 22 nous donne plusieurs pistes afin de le déterminer : il s'agit du lieu d'exercice d'une activité au moyen d'un dispositif stable.[191] C'est donc une notion de fait, à analyser au cas par cas.[192] Pour emprunter

---

[187] Deloitte Switzerland, « What do organisations need to do to show accountability for their data processing activities », disponible en ligne à l'adresse : https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-accountability-principle.html », consulté le 17 avril 2019.

[188] Article 25 du RGPD.

[189] Considérants 23 et 24 du RGPD.

[190] Article 3.1 du RGPD.

[191] « L'établissement suppose l'exercice effectif et réel d'une activité au moyen d'un dispositif stable. La forme juridique retenue pour un tel dispositif, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard », Identique au considérant 19 de la Directive.

[192] DE TERWANGNE, C., « Titre 2 - Définitions clés et champ d'application du RGPD », *op. cit.,* pp. 76 et s.

un terme au droit des sociétés, afin de remplir ce critère il faut que les potentiels débiteurs fassent preuve d'une certaine « substance » au sein de l'Union.

Dans l'arrêt Weltimmo[193], la Cour précise qu'un établissement même minime, en l'espèce la seule présence d'un représentant, peut suffire à remplir cette condition. Elle ajoute tout de même qu'un serveur ou un ordinateur ne pourraient pas être qualifiés de la sorte. C'est donc une interprétation large qui est donnée à la notion, qui se justifie par l'objectif de protection accru qui transcende le RGPD.[194]

§2 Pas d'établissement au sein de l'Union Européenne

Ensuite, le second critère a trait à l'absence d'établissement au sein de l'Union Européenne. C'est à ce sujet que le règlement fait preuve du plus d'innovation. En effet, les entreprises étrangères à l'Union Européenne ne cessent d'accroître leurs activités à destination des citoyens de l'Union. Ces règles concernent particulièrement les éditeurs d'applications, dont celles de *quantified self*, ayant généralement leur établissement hors Union. Par exemple, le service Strava se trouve aux États-Unis[195], il en va de même pour MyFitnessPal,[196] ou encore pour Runkeeper[197].

Il est dès lors, dans le cadre de ce propos, obligatoire de se questionner sur l'application du règlement à des sociétés résidentes hors de l'Union. Le RGPD a donc mis en place deux hypothèses permettant l'application des règles à ce type de sociétés.

A. Offre de biens ou de services au sein de l'Union Européenne

À partir du moment où le traitement de données personnelles par le responsable du traitement hors Union concerne la vente de biens ou la prestation de services, il y aura application du règlement pour ces traitements de données.[198]

---

193 C.J.U.E., 1er octobre 2015, arrêt *Weltimmo s.r.o. contre Nemzeti Adatvédelmi és Információszabadság Hatóság,*, C-230/14.

194 KINDT, E., « Why research may no longer be the same: about the territorial scope of the Proposed Data Protection Regulation » *CiTiP Working Paper*, n°26/2016, KU Leuven Centre for IT & IP Law, 2016, p. 12.

195 Les sites Web *Strava*, les applications mobiles et les services associés (collectivement, les « Services ») sont mis à votre disposition par Strava, Inc. dont le siège est sis au 208 Utah Street, San Francisco, CA 94103, États-Unis, disponible à l'adresse : https://www.strava.com/legal/terms?hl=fr-FR, consulté le 14 avril 2019.

196 Conditions générales de MyFitnessPal, disponible à l'adresse : « https://account.underarmour.com/fr-fr/privacy_and_terms# », consulté le 14 avril 2019.

197 Conditions générales de RunKeeper, disponible à l'adresse : « https://runkeeper.com/termsofservice », consulté le 14 avril 2019.

198 Article 3.2.a du règlement.

Il est précisé que l'application du règlement n'est subordonnée à aucune contrepartie en argent.[199] En effet, il est fréquent que des services soient offerts gratuitement à des utilisateurs qui fournissent leurs données au prestataire de service.

Le considérant 23 précise tout de même qu'il ne suffit pas que l'application ou le site en question soit accessible depuis un pays de l'Union. En effet, il est nécessaire que l'offre de biens ou de services soit dirigée vers l'Union, mais cela dépendra de critères factuels tels que la devise utilisée, la langue employée ou encore les disponibilités en termes de livraison.

À partir du moment où il sera possible de considérer que des services de *quantified self* sont dirigés vers l'Union comme par exemple avec un service de cartographie disponible dans l'Union, des langues parlées en son sein,… le règlement trouvera alors à s'appliquer même si la-dite application se base sur le modèle du *Freemium*.[200]

Par contre, lorsqu'un consommateur européen achète un produit sur le sol américain ou chinois, pendant ses vacances, et qu'il décide de le rapporter chez lui pour l'y utiliser alors que ce produit n'est pas destiné au marché européen, il est probable que ce produit ne soit pas conforme au RGPD.

B. Le suivi d'un comportement

En dernier lieu, l'application territoriale du RGPD dépend du suivi d'un comportement, pour autant que ce comportement ait lieu dans l'Union.[201] Le considérant 24 nous explique qu'il s'agit essentiellement de méthodes de profilage qui sont ainsi visées.[202]

Dans notre exemple du produit acheté à l'étranger, il est donc très probable que celui-ci ne fonctionne pas sur le sol européen car son utilisation emporterait application du RGPD pour le responsable du traitement américain ou chinois. Eu égard aux nombreuses obligations qui en découlent, on peut raisonnablement parier sur le non-fonctionnement de celui-ci.

---

[199] Considérant 23 du règlement.

[200] Voy. *supra*, Chapitre 1, Section 2, §3 Le quantified self en quelques chiffres.

[201] Article 3.2.b du règlement.

[202] Considérant 24 du règlement : Afin de déterminer si une activité de traitement peut être considérée comme un suivi du comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit.

Sous-Section 5. Conclusion intermédiaire

Au travers de cette analyse, nous remarquons que même si le RGPD a été présenté comme entièrement révolutionnaire, il conserve de nombreuses bases communes avec sa prédécesseur.[203] Les notions fondamentales de cette matière restent bien en place, fidèle à la vision qu'en avaient les auteurs de la Directive en 1992.

Le RGPD, toute comme la directive, se veut le plus large possible dans son application. Cette approche est cohérente avec la qualification de droit fondamental que reçoit la matière de la protection des données à caractère personnel. Les notions de "donnée", de "traitement" ou encore son champ d'application sont les plus inclusifs possibles afin de pouvoir suivre l'évolution fulgurante de la technologie. La matière des données personnelles se révèle donc particulièrement terre à terre, truffée de concepts nécessitant une application au cas par cas. Cela n'est pas sans poser de questions quant à la sécurité juridique amoindrie accompagnant ce type de technique légistique.

Quant aux figures permettant de légitimer le traitement, nous souhaitions mettre en exergue l'absence de pragmatisme du règlement dans la figure qu'il met en place. Cette définition, bien que très belle en théorie ne reçoit que peu d'application en pratique. Trop d'obstacles pratiques se dressent encore entre cette définition et la personne concernée. Cela pose dès lors de nombreuses questions quant à la possibilité de récolter des données sensibles dans le cadre du *quantified self* car la seule méthode envisageable dans ce domaine est la récolte du consentement explicite de la personne concernée.

Nous remarquerons tout de même une sérieuse évolution quant au champ d'application territorial du règlement. Une telle extension était nécessaire afin d'affirmer le caractère fort de cette matière sur le plan international et permet, désormais, de protéger l'ensemble des citoyens quant au traitement de leurs données personnelles par des responsables du traitement dispersés sur le globe.

[203] Notez qu'il n'existe pas de consensus quant au féminin de ce mot.

Chapitre 3. Contrôler ses données : utopie législative ou réalité ?

Après avoir analysé les principes règlementant la matière du *quantified self* ainsi que la matière de la protection des données à caractère personnel, nous étudierons un de ces domaines de manière plus pratique. Pour appréhender cette partie, nous démarrerons de l'hypothèse suivante : le règlement général sur la protection des données vise à octroyer un contrôle sur ses données à la personne concernée.[204]

Nous tâcherons donc en premier lieu de définir cette notion de contrôle pour ensuite analyser plusieurs dispositions du règlement pour déterminer si, dans le cadre du *quantified self* ici examiné, elles sont à même de donner le contrôle sur leurs données à la personne concernée. Enfin, nous clôturerons ce chapitre par une analyse des initiatives qui permettront peut être d'avancer face aux problèmes identifiés dans la section 2.

Section 1. Définition du contrôle

Tout d'abord, dans le sens commun, le contrôle se définit comme : « Action, fait de contrôler quelque chose, un groupe, d'avoir le pouvoir de les diriger ».[205]

En ce qui concerne la matière des données personnelles, le concept de contrôle résulte plutôt d'un choix restreint dans l'utilisation des données personnelles par un responsable du traitement. En effet, lorsque le traitement des données personnelles est basé sur l'hypothèse du consentement, plusieurs concepts viennent assurer que la personne concernée puisse faire un choix en ce qui concerne le traitement.[206] Par exemple, la granularité oblige le responsable du traitement à demander le consentement de la personne concernée pour chaque finalité de traitement, le droit de retrait garantit la possibilité de se retirer entièrement d'un service auquel il avait été consenti plus tôt, le droit à l'effacement est son corollaire lorsque plus aucune base légale ne justifie le traitement.[207]

---

[204] Considérant 7 du RGPD ; DE TERWANGNE, C., « Titre 2 - Définitions clés et champ d'application du RGPD », *op. cit.,* p. 102 ; C. LAZARO et D. LE METAYER, « Consent to Personal Data Processing: A Comparative Perspective on Data Subject's Autonomy », *op. cit.*, p. 802, 813 et 814.

[205] Définition du contrôle, disponible à l'adresse : « https://www.larousse.fr/dictionnaires/francais/contrôle/18932?q=controle#18822 », consulté le 21 avril 2019.

[206] Article 6.1 du RGPD.

[207] Articles 6.1.a, 7.3 et 17 du RGPD.

Malgré cela, plusieurs études prouvent que les consommateurs de services de *quantified self* ne ressentent pas ce sentiment de contrôle sur leurs données, malgré que 78% déclarent se soucier de ce qui est fait de leurs données. Ce sentiment est d'autant plus exacerbé par les pratiques des entreprises actives dans le domaine, nombreuses d'entre elles n'étant que peu respectueuses des règles en vigueur.[208]

Section 2. Analyse pratique de la portée du contrôle envisageable par la personne concernée

§1 La notion de consentement

A. Le consentement en général

Le consentement a été la source de nombreux abus sous l'empire de la Directive. Il était donc nécessaire de renforcer les exigences afin de lui permettre d'exister pleinement comme une base de légalisation du traitement de données.

Comme le soulignent de nombreux textes,[209] le consentement est un outil efficace pour légitimer le traitement de données à caractère personnel. Il doit permettre à la personne concernée de contrôler ses données à condition que celui-ci soit bel et bien conforme aux normes en la matière. Il est d'ailleurs le moyen le plus courant d'obtenir la légitimation du traitement et celui dans lequel les utilisateurs ont le plus confiance.[210] Cependant, très fréquentes sont les situations où le consentement est de qualité médiocre.

Comme le souligne très justement le groupe de l'article 29, le consentement n'est qu'une seule base du traitement des données. Il ne doit pas être vu comme source principale de légitimation du traitement et les autres hypothèses, tel le contrat, comme des solutions de repli, ce serait d'ailleurs

---

[208] Consumer Association of North Rhine-Westphalia , *Wearables and Fitness apps : data collection unchained,* 2017, disponible en ligne à l'adresse : « https://www.marktwaechter.de/sites/default/files/downloads/factsheet_0.pdf », consulté le 19 avril 2019 ; R. FAIRFIELD et H. MANN, *Quantified Self Report Card*, 2018, Human Data Commons Foundation, p.6, disponible l'adresse : « https://humandatacommons.org/wp-content/uploads/2018/11/HDC_RC_2018_FINAL.pdf », consulté le 15 avril 2018.

[209] Groupe de l'article 29, Lignes directrices sur le consentement au sens du règlement 2016/679, *op. cit.,* p. 3 ; Groupe de l'article 29, Avis 15/2011 sur la définition du consentement, *op. cit.*, p 11 ; C. LAZARO et D. LE METAYER, « Consent to Personal Data Processing: A Comparative Perspective on Data Subject's Autonomy », *op. cit.*, p. 801 ; C. DE TERWANGNE, « Titre 3 - Les principes relatifs au traitement de données à caractère personnel », *op. cit.,* p. 121.

[210] L. EDWARDS, « Privacy, security and data protection in smart cities: a critical eu law perspective. » *Eur Data Prot L Rev,* 2016, p. 28.

le contraire qui devrait être préconisé. Le consentement doit être plutôt vu comme une solution lorsque qu'aucune autre hypothèse n'est envisageable.[211]

Encore faut il que le consentement mis en exergue par le règlement puisse réellement exister. Les points suivants viennent appuyer ces différents arguments.

Tout d'abord, la première barrière au fait que la personne concernée puisse donner son consentement est que seulement très peu de personnes lisent les politiques de confidentialité des sites ou applications qu'elles utilisent. Une étude annonce que 91% des Américains ne liraient pas ces politiques, taux qui dépasse les 97% chez les 17-34 ans.[212] Dans le cadre du *quantified self*, une étude a démontré que seulement 18% des utilisateurs déclarent avoir lu la politique de confidentialité de leur outil.[213] De plus, dans une étude de 2008 par deux chercheuses de l'Université de Cannergie Mellon, il est annoncé que lire toutes les conditions générales des sites que l'on consulte prendrait en moyenne un mois chaque année.[214] Au vu du caractère relativement ancien de cette étude, nous ne pouvons imaginer ce que cela représenterait aujourd'hui. Tous ces faits nous éloignent encore un peu plus du consentement prévu par le règlement.[215]

Ensuite, selon le rapport de R. FAIRFIELD et H. MANN, trois paramètres doivent être pris en compte pour que la personne concernée puisse exercer un consentement tel qu'exigé par le règlement. Le consommateur doit être à jour avec le droit international afin de déterminer quelle loi est applicable à son contrat. En outre, celui-ci doit être particulièrement attentif à l'évolution de la technologie et des pratiques de commerce, une bonne compréhension du contexte global étant nécessaire pour en comprendre les implications. Enfin, il serait également de bon ton de relire régulièrement les politiques de vie privée mises en place par les applications envers lesquelles les données ont été transmises et légitimées par le biais du consentement, les mêmes qui étaient censées prendre un mois par an à lire en 2008.[216]

---

[211] Groupe de l'article 29, Lignes directrices sur le consentement au sens du règlement 2016/679, *op. cit.,* p. 3 ;

[212] Deloitte US, « Global Mobile Consumer Survey », 2017, p. 12, disponible en ligne à l'adresse : « https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/Global%20mobile%20consumer%20survey%20extended%20version.pdf », consulté le 19 avril 2019.

[213] D. LEIBENGER, F. MÖLLERS, A. PETRLIC, R. PETRLIC, et C. SORGE, « Privacy Challenges in the Quantified Self Movement – An EU Perspective », *Proceedings on Privacy Enhancing Technologies*, 2016 (4) , p. 326.

[214] A. MCDONALD et L. FAITH CRANOR, « The Cost of Reading Privacy Policies », *Journal of law and policy for the information society*, 2008, disponible en ligne à l'adresse : « https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf », consulté le 19 avril 2018.

[215] R. FAIRFIELD et H. MANN, *Quantified Self Report Card*, 2018, Human Data Commons Foundation, p. 6, disponible l'adresse : « https://humandatacommons.org/wp-content/uploads/2018/11/HDC_RC_2018_FINAL.pdf », consulté le 15 avril 2018.

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

De plus, lors de notre discussion avec Monsieur BAIJOT, celui-ci nous a confié qu'eu égard à sa fragilité, c'est un mécanisme qui a plus pour effet de protéger l'entreprise que l'utilisateur en lui même. L'utilisateur n'a pas de contrôle sur ses données à proprement parler car il n'a pas le choix d'accepter la politique de vie privée s'il veut utiliser l'application.[217]

Enfin, nous souhaitons remettre sérieusement en doute le fait que le consentement au traitement des données personnelles puisse être libre lorsqu'il concerne un rapport presque hégémonique de la part du prestataire sur la personne concernée. De nombreux responsables du traitement appartenant au monde du *quantified self* sont peu respectueux de la vie privée,[218] couplé au manque d'informations claires à destination du consommateur, nous pouvons raisonnablement établir un vrai rapport de force de la part d'une partie vis à vis de l'autre. Cependant, la disposition légale concernant cette présomption d'absence de consentement lors d'un tel rapport de force est trop peu précise : elle ne prévoit que trop peu d'exemples[219] et les termes de "déséquilibre manifeste" sont trop vagues et laissent une trop grande marge de manœuvre aux responsables du traitement.[220]

En ce qui concerne le considérant 32, nous souhaitions relever une phrase qui nous semblait incohérente avec l'économie du règlement. Alors que l'ensemble des dispositions du règlement semble préconiser une figure stricte du consentement, ce considérant déclare ceci : « Le consentement devrait être donné par un acte positif clair, […] cela pourrait se faire notamment en cochant une case lors de la consultation d'un site internet ». Cette déclaration a de quoi choquer car le simple fait de cocher une case sur un site internet n'a que peu très peu de chances de permettre une véritable prise de conscience sur le traitement des données, comme le règlement le laisse entendre.

Nous sommes donc particulièrement sceptiques sur la possibilité d'existence d'un consentement tel que celui mis en place par le règlement. Même si celui-ci est un idéal qui permettrait de légitimer le traitement des données, il est clair que celui-ci ne tient pas la route en pratique et ne devrait pas pouvoir légitimer un traitement de données, de surcroit sensibles dans le cadre du *quantified self*.

---

[217] Interview L. BAIJOT, Annexe, Question 6.
[218] *Ibid.*, p. 12, seuls trois responsables du traitement ont été classés avec des points positifs au sein de cette analyse.
[219] Considérant 43 du RGPD ; À savoir celui de l'employeur et de l'autorité publique.
[220] C. LAZARO et D. LE METAYER, « Consent to Personal Data Processing: A Comparative Perspective on Data Subject's Autonomy », *op. cit.*, p. 804.

B. La notion de consentement explicite au sein d'outils de quantified self

Afin de pouvoir légitimer un traitement de données sensibles telles que celles traitées par les outils de *quantified self*, il est nécessaire que l'utilisateur donne son consentement explicite au traitement de ses données.[221] En effet, le traitement des données sensibles est considéré comme interdit sauf lorsqu'une des hypothèses prévue est remplie.[222] De plus, les hypothèses de légitimation du traitement des données sensibles se révèlent plus restreintes que celles de leurs homologues ordinaires. Au sein des hypothèses de traitement des données sensibles ne figure pas une hypothèse du traitement de données sensibles dans le cadre de l'exécution d'un contrat.[223]

À partir du moment où nous doutons de la possibilité d'exercer un consentement tel que présent dans le règlement il n'est, selon nous, que probable qu'une personne concernée puisse consentir explicitement au traitement des données sensibles. Dès lors, dans la conjoncture actuelle, nous pouvons sérieusement douter de la légalité des activités des entreprises de *quantified self* au regard des règles relatives au traitement des données et, plus particulièrement, des données sensibles.

C. Le droit au retrait et à l'effacement

Le droit au retrait du consentement est, quant à lui, une expression claire du principe de contrôle des données à caractère personnel.[224] À partir du moment où une personne a le droit de donner librement son consentement, celle-ci devrait être habilitée à le retirer.[225] Ce mécanisme prévu à l'article 7.3 est un outil formidable qui permet à chacun, n'importe quand, de retirer son consentement sans aucun préjudice.[226] C'est-à-dire que lorsqu'un traitement de données sensibles ou ordinaires, est basé sur le consentement de la personne concernée, elle obtient le droit de retirer celui-ci pour n'importe quelle raison. C'est un droit octroyé à la personne concernée qui lui offre un contrôle sur ses données.

---

[221] La notion de consentement explicite aurait du figurer au sein des dispositions concernant les données ordinaires mais cette proposition n'a pas été retenue, à ce sujet voy. : P. DE HERT et V. PAPAKONSTANTINOU, « The new General Data Protection Regulation: still a sound system for the protection of individuals? », *Comp L & Security Rev.*, 2016, p.187, disponible en ligne à l'adresse : « https://pure.uvt.nl/ws/portalfiles/portal/19815940/pdh16_vpregulation_corrected_.pdf »,consulté le 21 avril 2019.

[222] Article 9 du RGPD.

[223] Article 9.2 du RGPD

[224] E. POLITOU, E. ALEPIS et C. PATSAKIS, « Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions », *op. cit.*, p. 7.

[225] L. CURREN et J. KAYE, « Revoking consent, a blind spot in data protection law ? », *Computer Law and security review*, 2010, pp. 273 à 283, disponible en ligne à l'adresse : « https://kundoc.com/pdf-revoking-consent-a-blind-spot-in-data-protection-law-.html », consulté le 21 avril 2019.

[226] Pour une analyse du retrait du consentement, voy. *supra* : Sous-Section 2. Le traitement, Paragraphe 4, A, pt. vii. Le retrait du consentement

D. Conclusion sur le consentement

Au regard de l'ensemble de l'analyse du consentement face aux outils de *quantified self,* nous souhaitions souligner que, dans l'état actuel des choses, ce concept n'est pas suffisamment abouti que pour pouvoir octroyer un réel contrôle sur leurs données aux personnes concernées. Malgré que cette notion soit très complète, les politiques de vie privée restent trop complexes et les enjeux trop difficiles à saisir pour pouvoir déclarer qu'un consentement a réellement été donné par la personne concernée. Le consentement n'est pas pour autant une notion à abandonner car il constitue le dernier rempart nous permettant de contrôler nos données.[227] C'est une notion particulièrement difficile à aborder car doivent être mis en balance deux intérêts divergents : d'une part, celui des personnes concernées qui doivent pouvoir être aptes à consentir pleinement au traitement de leurs données et de l'autre, celui des acteurs du *quantified self*, à qui il faut pouvoir offrir une base de traitement stable pour les données résultant de leur business.

§2 Le contrat

Le traitement de données personnelles peut, comme mentionné plus haut, être légitimé grâce à la méthode du contrat.[228] Pour revenir succinctement sur cette notion, à partir du moment où le traitement des données en question est nécessaire à l'exécution du contrat, aucun consentement de la part de la personne concernée ne sera nécessaire.[229]

C'est donc une méthode de légitimation du traitement sur laquelle la personne concernée n'aura aucun contrôle sur ses données. En effet, à partir du moment où les données rentrent dans l'exécution nécessaire du contrat, les données pourront être traitées par le responsable du traitement, même si la personne concernée s'y oppose.

§3 Les pratiques au sein des entreprises actives dans le quantified self

Malgré que les personnes concernées soient en partie responsables de ne pas lire les politiques de vie privée, nous souhaitons mettre en exergue les pratiques des entreprises actives dans le domaine du *quantified self.* Elles sont souvent peu respectueuses des droits des utilisateurs en matière de

---

[227] P. DE HERT et V. PAPAKONSTANTINOU, « The new General Data Protection Regulation: still a sound system for the protection of individuals? », *op. cit.* p. 187.
[228] Article 6.1.b du RGPD ; Voy. Chapitre 2, Section 2, Sous-Section 2, §4, B, Le contrat.
[229] Groupe de l'article 29, Avis 06/2014, *op. cit.* p. 18.

données à caractère personnel, profitant de leur crédulité pour leur faire accepter des politiques de confidentialité exorbitantes.

Tout d'abord, en ce qui concerne le traitement des données, seuls très peu de services de *quantified self*[230] laissent le choix aux personnes concernées de décider où seront stockées les données, c'est-à-dire soit sur les serveurs de l'entreprise ou sur l'appareil de l'utilisateur.[231]

Ensuite, quatre services de *quantified self* sur les huit analysés l'étude de D. LEIBENGER rendent publiques par défaut les données des personnes concernées présentes sur leur application.[232]

De plus, même s'il est nécessaire que les utilisateurs donnent accès à leurs données à caractère personnel pour l'utilisation de l'application ou du traqueur, les entreprises en profitent souvent afin de s'autoriser l'utilisation des données pour d'autres finalités que celles-ci afin de se garantir des droits en plus. En outre, seuls trois de ces huit prestataires notifieront à l'utilisateur si la politique de confidentialité est modifiée.[233]

Enfin, l'analyse de R. FAIRFIELD et H. MANN, ne fait que confirmer ces observations. Lors de leur étude complète portant sur les politiques de vie privée de 45 entreprises actives dans le quantified self, seules 16 obtiennent un score positif. De plus, excepté les quatre premières entreprises, elles peuvent toutes être épinglées pour des mauvaises pratiques concernant soit les droits des utilisateurs, soit les conditions de stockage des données, soit encore pour des transmissions non autorisées de données à des tiers.[234]

§4 Conclusion intermédiaire

En définitive, nous pouvons déplorer le manque de contrôle donné à la personne concernée sur ses données. Le consentement est une notion hautement critiquable, car pas assez abouti que pour donner un réel contrôle, intrinsèquement, le contrat ne le permet pas non plus et les pratiques au sein du marché posent de nombreuses questions. Cette conclusion est particulièrement décevante lorsque l'on sait que ce contrôle est un des objectif affiché du règlement et que ces données peuvent s'avérer sensibles.

---

230 Notamment Runtastic qui offre le choix de stocker les données en local sur l'appareil de l'utilisateur.
231 D. LEIBENGER, F. MÖLLERS, A. PETRLIC, R. PETRLIC, et C. SORGE, « Privacy Challenges in the Quantified Self Movement – An EU Perspective », *op. cit*, p. 321.
232 *Ibid*., p. 322.
233 *Ibid*., p. 323.
234 R. FAIRFIELD et H. MANN, *Quantified Self Report Card*, *op. cit.*, p. 3.

Section 3. Initiatives tierces au règlement afin de rendre le contrôle de leurs données aux personnes concernées

Par cette section, nous souhaitions présenter quelques initiatives prenant place hors du règlement qui ont pour idéal de rendre le contrôle sur leurs données aux personnes concernées.

§1 Repenser les politiques de vie privée

Plutôt que d'insister sur l'ignorance des personnes concernées, il est également possible de mettre en cause la clarté des politiques de vie privée des entreprises actives dans le *quantified self*. Il serait possible d'obtenir un meilleur consentement avec des supports plus lisibles. On remarque que celles-ci sont très souvent mal informées sur des informations qu'elles estiment essentielles : plusieurs chercheurs ont réalisé une étude au cours de laquelle ils demandaient à des utilisateurs de *quantified self* s'ils savaient que certaines données étaient traitées pour, ensuite, leur demander s'ils comptaient arrêter d'utiliser cet outil à cause du traitement des données en cause. Une majorité d'entre eux n'était pas au courant de l'utilisation de leurs données à caractère personnel dans des buts de profilage et souhaitent donc arrêter de l'utilisation du service pour ces raisons. Cette étude montre donc à quel point les utilisateurs sont peu informés par ces politiques de confidentialité.[235]

Il est vrai que le RGPD donne comme obligation au responsable du traitement de fournir une politique de confidentialité simple et compréhensible.[236] Cependant, ces documents sont rédigés pour satisfaire aux conditions du règlement et non pour la compréhension des utilisateurs[237]

Une piste dans ce sens est que les longs documents comportant plusieurs sections et paragraphes devraient être bannis, ils sont peu attrayants et comportent généralement trop d'informations pour la personne concernée. Il serait plus judicieux de ne donner que les informations nécessaires et de les adapter en fonction de la personne concernée, par exemple en les divisant en parties plus restreintes qui s'afficheraient au moment opportun. Il y aurait une première acceptation de la politique lorsque l'on commence à utiliser le service. Ensuite, chaque fois qu'une fonctionnalité serait utilisée, un

---

[235] D. LEIBENGER, F. MÖLLERS, A. PETRLIC, R. PETRLIC, et C. SORGE, « Privacy Challenges in the Quantified Self Movement – An EU Perspective », *op. cit.*, p. 327.

[236] Considérant 42 du RGPD ; Articles 7.2, et 12.7 du RGPD.

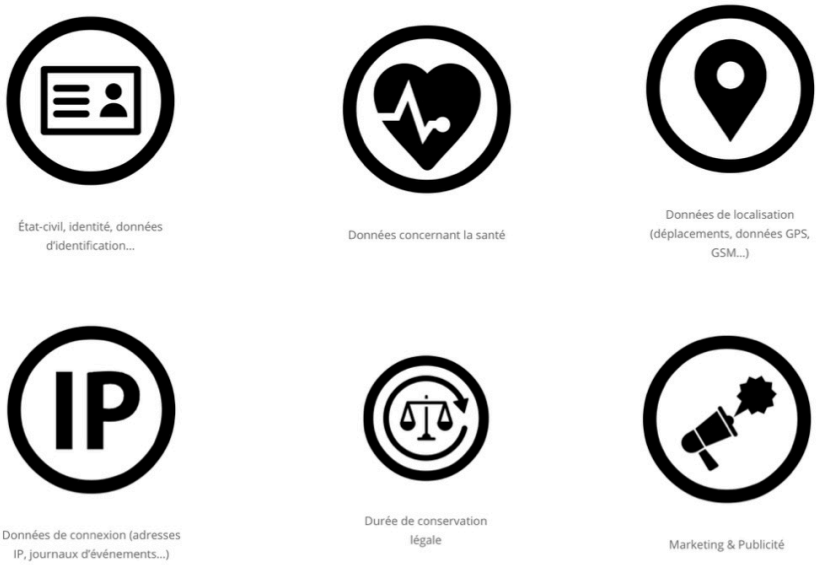
[237] F. SCHAUB, « Nobody reads privacy policies – here's how to fix that », The Conversation, 2017, disponible en ligne à l'adresse : « http://theconversation.com/nobody-reads-privacy-policies-heres-how-to-fix-that-81932 », consulté le 21 avril 2019.

message s'afficherait afin de savoir si la personne concernée accepte le traitement des données pour cette fonctionnalité.[238]

Le considérant 42 du RGPD donne de bonnes pistes pour rendre ces documents plus lisibles : il préconise l'utilisation d'icônes afin de permettre une meilleure compréhension. C'est notamment l'objet d'une recherche menée par un groupe de travail du navigateur Mozilla qui avait pour but d'utiliser des icônes que l'on pourrait placer directement sur les sites ou sur les applications afin de savoir rapidement quel était l'utilisation des données.[239]

Plus récemment, le site PrivacyTech a également mis sur pied un projet similaire visant à actualiser cette initiative mise en place par Mozilla en 2011. Les icônes développées par Mozilla ont été actualisées à l'aide des concepts du règlement. Il y a notamment une icône qui indique que l'application en question réalise du profilage à l'aide des données collectées, ou une autre qui indique que l'application collecte des données sensibles,… Cela pourrait représenter un avantage concurrentiel certain pour les entreprises mettant en avant des icônes respectant la vie privée.

À travers ces icônes simples, la personne concernée se replace au centre du contrôle de ses données, elle peut déterminer bien plus aisément si le prestataire en question est respectueux de sa vie privée. En voici quelques exemples particulièrement pertinents dans ce cadre :



[238] F. SCHAUB, « Nobody reads privacy policies – here's how to fix that », *op. cit.* ; F. SCHAUB, R. BALEBAKO, A. L. DURITY, L. FAITH CRANOR, « A Design Space for Effective Privacy Notices », Symposium on Usable Privacy and Security, 2015, p. 326, disponible à l'adresse : « https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf », consulté le 21 avril 2019.
[239] A. RASKIN, Privacy Icons, disponible en ligne à l'adresse : « https://wiki.mozilla.org/Privacy_Icons », consulté le 21 avril 2019.

Lors de notre discussion avec L. BAIJOT, nous avons discuté de l'idée d'implanter ce type d'icônes au sein d'une application de *quantified self* telle que celle de son entreprise. Il estime que ce type d'initiative serait une avancée en termes de consentement au traitement des données donné par la personne concernée.

Il a également émis l'idée de pouvoir se servir de ces icônes comme portails interactifs au travers desquels il serait possible de gérer les traitements correspondants à l'icône sélectionnée. En clair, pour gérer le traitement de données concernant la santé, la personne concernée n'aurait qu'à appuyer sur l'icône représentant un coeur, ce qui lui ouvrirait une page lui expliquant clairement le traitement de ces données et lui donnant l'occasion d'en autoriser le traitement ou pas. Cette innovation aurait également pour effet de renforcer la granularité du consentement.[240]

§2 Le self data

A. Notion

Une autre solution permet d'aller bien plus loin que d'informer la personne concernée. Le mouvement du *self data* a été initié en France par la Fondation Internet Nouvelle Génération (FING),[241] au Royaume-Uni par le Gouvernement via *MiData*[242] et aux États-Unis par diverses initiatives telles que le *blue* et le *green button*.

Cette incise concernant le *self data* n'est qu'une introduction au sujet et ne prétend ici à aucune exhaustivité au vu de la quantité de questions tant théoriques que pratiques que cette matière pose. Nous veillerons donc uniquement à l'introduire en guise de solution future pour une meilleure gestion des données par les personnes concernées.

Selon la FING, le *self data* désigne « la production, l'exploitation et le partage de données personnelles par les individus, sous leur contrôle et à leurs propres fins. Le Self Data, c'est devenir acteur de ses données personnelles. Ne plus se contenter de les produire pour que d'autres les exploitent (à des fins marketing par exemple), mais bien récupérer la maîtrise de celles-ci. »[243]

---

[240] Interview L. BAIJOT, Annexe, Question 7.
[241] Voy. not. : http://mesinfos.fing.org/selfdata-2/
[242] Voy. not. : https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment
[243] FING, *Comprendre le self data, FAQ version 1,* 2016, p. 3, disponible en ligne à l'adresse : « http://mesinfos.fing.org/wp-content/uploads/2015/07/FAQ_SELFDATA_V1.pdf », consultée 16 mai 2019.

C'est donc un courant de pensée qui vise à rendre le pouvoir sur leurs données personnelles aux personnes concernées. Ces données sont aujourd'hui particulièrement difficiles d'accès car elles se trouvent au sein des serveurs des entreprises. L'idée défendue par la FING est que ce soient les utilisateurs eux mêmes qui stockent leurs données sur des *Personnal Information Management Systems* (PIMS), qui sont des services de cloud ultra sécurisés et dédiés à une seule personne.[244]

C'est en quelque sorte l'opposé du *BigData*, qui implique la détention des données par les entreprises pour servir leurs propres besoins commerciaux. Le *self data* a comme ambition que chacun possède ses propres données et puisse les gérer lui-même, éventuellement avec l'aide de partenaires de confiance.[245]

Au sein de cette base de données détenue par la personne concernée elle-même, pourraient figurer les données récoltées par des services de *quantified self*. Chaque utilisateur d'un tel outil pourrait récolter lui-même les données pour les communiquer à qui il le souhaite.[246] Par exemple, il pourrait choisir de mettre à disposition de son médecin les données récoltées par ses dispositifs de *quantified self*.

Selon nous, une telle initiative reste fort avant-gardiste mais a tout de même le mérite d'avancer dans l'optique de donner du contrôle à l'utilisateur sur ses données.

B. Le Blue Button

Le *blue button est un projet américain* qui se situe dans la continuité du *self data*. C'est une initiative qui permettrait de donner du contrôle sur leurs données de santé aux utilisateurs d'outils de *quantified self*.

Ce projet a, à l'origine, été développé pour les citoyens américains afin d'accéder à leurs données de santé d'un seul clic. C'est une application et un site internet qui permettent aux personnes concernées d'alimenter eux mêmes leurs données au sein d'une plateforme sécurisée. Cette alimentation peut être faite notamment via des données récoltées par des dispositifs de *quantified self*. De là, ils peuvent choisir de partager tout ou partie de ces données en autorisant l'accès à cette application à qui ils le souhaitent. Cela peut par exemple être le médecin, la pharmacie, la

---

[244] *Ibid.* p. 3.
[245] *Ibid.* pp. 3 et 4.
[246] *Ibid.* p. 5.

compagnie d'assurances,…[247] Ils peuvent ensuite recevoir un récapitulatif de ces données sous la forme d'un document texte pour savoir quelles données ils ont renseigné et à qui ils ont donné accès.[248]

Cette initiative a été mise en oeuvre en premier par plusieurs ministères américains (défense, vétérans, santé et services sociaux). Ensuite, les pharmacies, les laboratoires, les prestataires de services médicaux et les compagnies d'assurances ont franchi le pas.

Cette initiative américaine est également portée, de notre coté de l'Atlantique, et plus particulièrement en France par la (FING). Malgré que ce projet s'inscrive dans un contexte majoritairement médical sortant de notre propos, son articulation évidente avec les dispositifs de *quantified self* le rend pertinent dans ce cadre.[249]

Le but principal de ce projet et de donner à la personne concernée une autonomie informationnelle, en développant un fichier standardisé permettant d'être réutilisé d'un prestataire de services à l'autre.[250] Les données provenant de dispositifs de *quantified self* pourraient être intégrées de sorte que les prestataires qui pourraient avoir besoin de ces données puissent y avoir accès aisément.

Cette méthode permettrait de regrouper en un seul endroit toutes les données concernant la santé de la personne concernée. Cela lui permettrait de reprendre, du moins en partie, le contrôle sur ses données de santé transmises aux applications de *quantified self*.[251]

Selon nous, un tel dispositif pourrait permettre aux personnes concernées de prendre conscience de l'usage qui est fait de leurs données et pourquoi pas de sauter le pas vers une mise en place de dispositifs de *self data* pour gérer leurs informations de santé.

---

[247] H. AZIZ et M. MOHSEN, « The Blue Button Project: Engaging Patients in Healthcare by a Click of a Button », Perspectives in health information management, American Health Information Management Association, 2015, p. 1, disponible en ligne à l'adresse : « https://www.researchgate.net/publication/312653302 », consulté le 12 mai 2019 ; D. FRIDSMA, « Health IT Standards Committee Update », *Office of the National Coordinator for Health Information Technology*, 2012, disponible en ligne à l'adresse : « http://www.healthit.gov/sites/default/files/hitsc_nov13_2012_fridsma.pdf », consulté le 12 mai 2019.

[248] H. AZIZ et M. MOHSEN, « The Blue Button Project: Engaging Patients in Healthcare by a Click of a Button », *op. Cit*, p. 2.

[249] M. ALBARÈDE et M. MOLINS, *Mes infos santé, vers un blue button à la française*, 2016, disponible en ligne à l'adresse : « http://mesinfos.fing.org/wp-content/uploads/2016/05/MesInfos_Sante_Pages.pdf », consulté le 16 mai 2019.

[250] *Ibid.,* p. 20.

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

Conclusion

Afin de clore cette contribution, nous souhaitions revenir sur les quelques questions que nous nous étions posées en introduction : Quels sont ces appareils qui font partie du *quantified self* ? Quelles sont les données collectées par ces appareils ? Sommes-nous capables de donner notre consentement au traitement de ces données ? Qu'en dit la loi ? Les concepts mis en place sont-ils suffisants pour protéger les utilisateurs, et le cas échéant, que peut on faire pour y pallier ?

Tout d'abord, en ce qui concerne les appareils de *quantified self*, nous avons pu voir qu'il en existe une multitude. Cela peut aller de l'application sportive à celle sur l'humeur en passant par le sommeil. De nombreux traqueurs, bracelets ou montres, sont également présents sur le marché. En effet, c'est un marché lucratif et en pleine expansion pour les entreprises qui les produisent.

Ensuite, les données collectées par ces outils sont nombreuses : informations personnelles de base pour l'inscription, données de localisation pour la pratique d'activités, données relatives à la santé lorsque l'on traque son rythme cardiaque,…

La question du consentement nous aura, quant à elle, retenu plus longtemps. Nous sommes d'avis que chaque personne concernée n'est aujourd'hui pas en capacité de pouvoir donner son consentement au traitement des données personnelles tel que réalisé par les applications de *quantified self*. Même si elle est une pierre angulaire du traitement des données personnelles et doit le rester, elle doit être soutenue par d'autres outils permettant d'en assurer un fonctionnement efficace.

Enfin, en ce qui concerne les outils susceptibles d'aider à la construction d'un consentement fort, nous souhaitions mettre en avant deux initiatives d'ambition différente. L'implémentation d'icônes sur le traitement de données nous parait envisageable à court terme. Le *self data* nous semble plus un travail de longue haleine, résultant d'un travail de sensibilisation bien plus fort. Il n'empêche que de nombreuses initiatives dans cet esprit, seront nécessaires afin de pouvoir donner un contrôle sur leurs données aux personnes concernées par le traitement de données réalisé par des outils de *quantified self*.

C'est donc une cohabitation difficile qui s'annonce entre les acteurs du *quantified self* et le RGPD. En effet, comme nous avons pu le démontrer au sein de ce mémoire, la base légale, permettant de légitimer le traitement des données personnelles sensibles ou non récoltées par des outils de

quantified self, est fragile. Cette idée a d'ailleurs été confirmée par notre précieuse interview avec Monsieur BAIJOT. Comme nous l'ont montré plusieurs études, les politiques de vie privée de ces entreprises restent encore trop favorables à celle-ci. De plus, les pratiques de ces mêmes entreprises laissent encore, pour nombre d'entre elles, à désirer.

Il reste donc du chemin à parcourir pour que les utilisateurs d'outil de *quantified self* soient conscients de l'enjeu que représente leurs données personnelles et donc, qu'ils en obtiennent le contrôle. Malgré cela, nous ne pouvons que soutenir des initiatives telles que celles de la FING ou celles de ThePrivacyTech.

En effet, lorsque l'on constate l'état de la matière ainsi que les outils mis en place par le RGPD, il est normal que l'on voit émerger des doctrines prêchant pour une possession des données personnelles par les utilisateurs.

Il est d'ailleurs tout aussi indispensable de prévoir des méthodes permettant d'offrir une meilleure information aux utilisateurs. En effet, une connaissance améliorée des enjeux sera bénéfique pour les deux parties : d'une part, cela permettra à l'utilisateur de comprendre ce qui l'entoure et les conséquences de ses choix en matière de données personnelles. D'autre part, pour les entreprises, cette information accrue permettra non seulement de donner une réelle force au consentement en tant que mode de légitimation du traitement mais aussi de donner confiance aux utilisateurs.

Bibliographie

Doctrine

1. AJANA, B., « Digital health and the biopolitics of the quantified self », *Digital Health*, Londres, 2017, Vol. 3., disponible en ligne à l'adresse : https://www.researchgate.net/publication/312090206_Digital_Health_and_the_Biopolitics_of_the_Quantified_Self, consulté le 19 février 2019.

2. ALBARÈDE, M., et MOLINS, M., *Mes infos santé, vers un blue button à la française*, 2016, disponible en ligne à l'adresse : « http://mesinfos.fing.org/wp-content/uploads/2016/05/MesInfos_Sante_Pages.pdf », consulté le 16 mai 2019.

3. ALEPIS, E., POLITOU, E. et C. PATSAKIS, C., « Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions », *Journal of cyber security*, 2018, Department of Informatics, University of Piraeus, Piraeus, p. 5, disponible en ligne à l'adresse : « https://tinyurl.com/Forgettingpersonaldata », consulté le 21 avril 2019.

4. ARRUABARRENA, B., *Le Soi augmenté : les pratiques numériques de quantification de soi comme dispositif de médiation pour l'action*, Sciences de l'information et de la communication, Conservatoire national des arts et métiers - CNAM, 2016, p. 16.

5. AZIZ, H. et MOHSEN, M., « The Blue Button Project: Engaging Patients in Healthcare by a Click of a Button », *Perspectives in health information management, American Health Information Management Association*, 2015, disponible en ligne à l'adresse : « https://www.researchgate.net/publication/312653302 », consulté le 12 mai 2019.

6. BATHELOT, B., La définition d'une application mobile, 2017, disponible sur : https://www.definitions-marketing.com/definition/application-mobile/, consulté le 17 mars 2019.

7. BBC News, « Calorie burner: How much better is standing up than sitting? », *BBC Website*, disponible en ligne à l'adresse : « https://www.bbc.com/news/magazine-24532996 », consulté le 9 avril 2019.

8. BERMINGHAM-MCDONOGH, N., *The data science of the quantified self*, 2015, Vrije Universiteit Amsterdam, p. 8.

9. BIRKAVS, E., KOEDIJK, M., MING, X. et WOLBERS, B., *The Quantified Self - Self-knowledge Through Numbers?*, Twente, Technolab, 2017, p. 2, disponible en ligne : http://www.ideefiks.utwente.nl/wp_base/wp-content/uploads/2016/01/Final-Project-Quantified-Self-6_22_2016.pdf, consulté le 16 février 2019.

10. CASSART, A., CATTEAU, A., COTON, F., DELCOMINETTE, S., ERNOTTE, F., HAMBLENNE, N., LIMBRÉE, P., RONNEAU, V. et VAN DEN BRANDEN, A., *Le droit des Machintechs (FinTech, Legal Tech, MecdTech,…), État des lieux et perspectives*, Bruxelles, Larcier, Coll. Jeune Barreau du Brabant Wallon, 2018.

11. Centre Canadien d'hygiène et de sécurité au travail, La marche, toujours le meilleur remède, disponible en ligne à l'adresse : « https://www.cchst.ca/oshanswers/psychosocial/walking.html », consulté le 9 avril 2019.

12. Consumer Association of North Rhine-Westphalia , « Wearables and Fitness apps : data collection unchained », 2017, disponible en ligne à l'adresse : « https://www.marktwaechter.de/sites/default/files/downloads/factsheet_0.pdf », consulté le 19 avril 2019

13. COOPER B.B., « Is 10,000 steps really the best measurement of our health? », *The Next Health*, 2013, http://thenextweb.com/apps/2013/11/29/10000-steps-really-best-measurement-health/#gref, consulté le 30 mars 2019.

14. CRAWFORD, K., *Our metrics, ourselves: A hundred years of self- tracking from the weight scale to the wrist wearable device*, 2015, *Eur J Cultural Studies,* pp. 18 et s.

15. CRAWFORD, K., « When Fitbit Is the Expert Witness », *The Atlantic*, 2014, disponible en ligne à l'adresse « https://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936/ », consulté le 9 avril 2019.

16. CURREN, L., et KAYE, J., « Revoking consent, a blind spot in data protection law ? », *Computer Law and security review*, 2010, pp. 273 à 283, disponible en ligne à l'adresse : « https://

kundoc.com/pdf-revoking-consent-a-blind-spot-in-data-protection-law-.html », consulté le 21 avril 2019.

17. DELFORGE, A., « Les obligations générales du responsable du traitement et la place du sous-traitant », *Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Éditions Larcier, 2018, pp. 371 à 407.

18. Deloitte US, « Global Mobile Consumer Survey », 2017, p. 12, disponible en ligne à l'adresse : « https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/Global%20mobile%20consumer%20survey%20extended%20version.pdf », consulté le 19 avril 2019.

19. DEMOULIN, M., *Droit des contrats à distance et du commerce électronique*, Waterloo, Kluwer, 2010, p.107.

20. DESROSIÈRES, A., « Pour une sociologie historique de la quantification », *L'argument statistique I*, 2008, Presses de l'École des mines, p. 10 et 11.

21. DE SOUZA, P., Self-tracking and body hacking: The biopolitics of the Quantified Self in the age of neoliberalism, disponible en ligne à l'adresse : « https://bodycartography.wordpress.com/2013/06/11/self-tracking-and-body-hacking-the-biopolitics-of-the-quantified-self-in-the-age-of-neoliberalism », consulté le 17 mars 2019.

22. DE TERWANGNE, C., « Titre 2 - Définitions clés et champ d'application du RGPD », *Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Éditions Larcier, 2018, pp. 59 à 84.

23. DE TERWANGNE, C., « Titre 3 - Les principes relatifs au traitement de données à caractère personnel », *Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Éditions Larcier, 2018, pp. 87 à 142.

24. DE TERWANGNE, C., « La difficile application de la législation de protection des données à caractère personnel. obs. sous Cass. (belge) 22 février 2017 », *J.T.*, 2017, pp. 752 et s.

25. DOW SCHÜLL, N., Self in the loop : « Bits patterns, and pathways in the quantified self », *The Networked Self*, 2018, New York, Vol 5: Human Augmentics, Artificial Intelligence, Sentience, Ed. Zizi Papacharisi pp. 25 et s.

26. DRAPER S., « Pentagon Tells Soldiers to Leave Wearable Trackers at Home When Heading to Warzones », 9 aout 2018, disponible à l'adresse : « https://www.wearable-technologies.com/2018/08/pentagon-tells-soldiers-to-leave-wearable-trackers-at-home-when-heading-to-warzones/ », consulté le 15 avril 2019.

27. EDWARDS, L., « Privacy, security and data protection in smart cities: a critical eu law perspective. » *Eur Data Prot L Rev,* 2016, p. 28.

28. European Data Protection Supervisor, « Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content », 14 mars 2017, p. 18.

29. European Data Protection Supervisor, « Accountability », disponible en ligne à l'adresse : « https://edps.europa.eu/data-protection/our-work/subjects/accountability_en »,consulté le 17 avril 2019.

30. FRIDSMA, D., « Health IT Standards Committee Update », *Office of the National Coordinator for Health Information Technology*, 2012, disponible en ligne à l'adresse : « http://www.healthit.gov/sites/default/files/hitsc_nov13_2012_fridsma.pdf », consulté le 12 mai 2019.

31. Groupe de l'article 29, Avis 4/2007 sur le concept de données à caractère personnel, WP 136, 20 juin 2007, disponible en ligne à l'adresse : « https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf », consulté le 12 avril 2019.

32. Groupe de l'article 29, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », WP 169, p.9, disponible en ligne à l'adresse : « http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf », consulté le 20 mars 2019.

33. Groupe de l'article 29, Avis 15/2011 sur la définition du consentement, WP 187, 13 juillet 2011, disponible en ligne à l'adresse : « https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp187_fr.pdf », consulté le 16 avril 2019.

34. Groupe de l'article 29, Opinion 03/2013 on purpose limitation, 2 avril 2013, disponible en ligne à l'adresse : « https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp203_en.pdf », consulté le 16 avril 2019.

35. Groupe de l'article 29, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE , WP 217, 9 avril 2014, disponible en ligne à l'adresse : «https://www.alain-bensoussan.com/wp-content/uploads/2016/09/20140409.pdf », consulté le 17 avril 2019.

36. Groupe de l'article 29, Avis 8/2014 sur les récentes évolutions relatives à l'internet des objets, WP 223, 16 septembre 2014, pp. 6, 7 et 17, disponible en ligne à l'adresse : « https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp223_en.pdf », consulté le 17 avril 2019.

37. Groupe de l'article 29, Lignes directrices sur le consentement au sens du règlement 2016/679,WP 269 rév.1 ,10 avril 2018, disponible en ligne à l'adresse : « https://www.cnil.fr/sites/default/files/atoms/files/ldconsentement_wp259_rev_0.1_fr.pdf », consulté le 16 avril 2019.

38. GOBRY, P.-E., *Explainer: What Is The Freemium Business Model?*, 2011, disponible en ligne à l'adresse : « https://www.businessinsider.com/what-is-the-freemium-business-model-2011-4?IR=T », consulté le 27 mars 2019.

39. HILTS, A., PARSONS, C., et KNOCKEL, J., *Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security*, 2016, Open Effect Report (2016), disponible sur : https://openeffect.ca/reports/Every_Step_You_Fake.pdf, consulté le 17 mars 2019.

40. HOY, M., *Personal activity trackers and the Quantified Self*, Eau Claire, 2016, Vol. 35, n°1, pp. 94 à 100.

41. HUOTARI, K. et HAMARI, J. « A definition for gamification: anchoring gamification in the service marketing literature », *Electronic Market*s, 2017, n°27/1, pp. 21 à 31.

42. Information Commissioner's Office, *Consultation: GDPR consent guidance*, 30 mars 2017, disponible en ligne à l'adresse : « https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf », consulté le 17 avril 2019.

43. KELLY, K., dans TAKASHI D., Quantifiying our lives will be a top trend in 2012, article en ligne, disponible sur « https://venturebeat.com/2012/01/21/quantifying-our-lives-will-be-a-top-trend-of-2012/ », consulté le 13 mars 2019.

44. KINDT, E., « Why research may no longer be the same: about the territorial scope of the Proposed Data Protection Regulation » *CiTiP Working Paper*, n°26/2016, KU Leuven Centre for IT & IP Law, mai 2016.

45. KUMAR, V., « Making Freemium Work », *Harvard Business Review*, 2014, disponible à l'adresse : « https://hbr.org/2014/05/making-freemium-work », consulté le 27 mars 2019.

46. LAURENT, J., « Healthscapes of self-quantification : Quantifying, knowing and improving one's self: transforming health » in eä Journal, 2015, Vol. 7 N° 1, p. 111.

47. LAZARO, C., et LE METAYER, D., « Consent to Personal Data Processing: A Comparative Perspective on Data Subject's Autonomy », *R.J.T.,* 2014, disponible en ligne à l'adresse : « http://heinonline.org/HOL/Index?index=journals/revjurns&collection=journals », consulté le 16 avril 2019.

48. LECLERCQ, T., PONCIN, I., HAMMEDI, W. et KULLAK, A., *Effects of Gamification on Customer Engagement in Online Communities,* Louvain Research Institute in Management and Organizations Working Paper Series, 2018, n°10.

49. LEE, V., « What's Happening in the "Quantified Self" Movement ? », *Instructional Technology and Learning science Faculty publications,* 2014*,* Utah*,* n°491, pp. 1032 et s.

50. LEIBENGER, D., MÖLLERS, F.,PETRLIC, A., PETRLIC, R. et SORGE, C., « Privacy Challenges in the Quantified Self Movement – An EU Perspective », *Proceedings on Privacy Enhancing Technologies*, 2016 (4) , pp. 315 à 334.

51. LUPTON, D., « Quantified sex : a critical analysis of sexual and reproductive self tracking using apps », in *Cult Health sex*, 2014, n°17, pp. 1 à 14.

52. MACIULIENE, M., et SKARZAUSKIENE, A, « Evaluation of co-creation perpective in networked collaboration platforms » *Journal of Business Research,* 2016/69, pp. 4826 à 4830.

53. MOINY, J.-Ph., « Are Internet protocol addresses personal data ? the fight against online copyright infringement », C.L.S.R./27, 2011, pp. 348 à 361.

54. NINI, J., « How Wearable Technology is Making It's Way into the Courtroom », *Smith Lawyers' Blog*, 2018, disponible à l'adresse : https://www.smithslawyers.com.au/post/wearable-technology-courtroom, consulté le 30 mars 2019.

55. OLSON, P., « FitBit data now used in court room », *Forbes*, 2014, disponible à l'adresse : « https://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/#2862ec177379 », consulté le 30 mars 2019.

56. Rocket fuel, *"Quantified Self " digital tools a cpg marketing opportunity*, 2014, pp. 1 à 12, disponible sur : http://quantifiedself.com/docs/RocketFuel_Quantified_Self_Research.pdf consulté le 21 mars 2019.

57. ROUVROY, A., « Avant-Propos », in *CNIL, Le corps, nouvel objet connecté, du quantified self à la m-santé : les nouveaux territoires de la mise en donnée du monde, Cahiers IP, n°2*, 2014, p. 4 disponible sur : https://www.cnil.fr/sites/default/files/typo/document/, consulté le 21 mars 2019.

58. ROSIER, K., FIEVET, C., GERARD, L., VANRECK, O., MICHEL, A., MONT, J., KNOCKAERT, M., GILLARD, N. et TOMBAL, T., « Droit au respect de la vie privée et à la protection des données en lien avec les technologies de l'information - Chronique de jurisprudence 2015-2017 », *R.D.T.I.*, 2017/3-4, n° 68-69, p. 94 à 163.

59. ROWSE LM. « Statistics of the self: Shaping the self through quantified self-tracking. » *Scripps Senior Thesis*, Claremont Colleges, USA, 2015, p. 49, disponible à l'adresse : « https://scholarship.claremont.edu/cgi/viewcontent.cgi?article=1656&context=scripps_theses », consulté le 30 mars 2019.

60. SCHAUB, F., « Nobody reads privacy policies – here's how to fix that », *The Conversation*, 2017, disponible en ligne à l'adresse : « http://theconversation.com/nobody-reads-privacy-policies-heres-how-to-fix-that-81932 », consulté le 21 avril 2019.

61. SCHAUB, F., BALEBAKO, R., DURITY, A. L. et FAITH CRANOR, L., « A Design Space for Effective Privacy Notices », Symposium on Usable Privacy and Security, 2015,disponible à l'adresse : « https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf », consulté le 21 avril 2019.

62. SHARON T. *Self-tracking for health and the quantified self: Re-articulating autonomy, solidarity, and authenticity in an age of personalized healthcare*, 2016, Philos Technology, p. 129.

63. VAN GYSEGHEM, J.-M., « Les catégories particulières de données à caractère personnel », *Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Éditions Larcier, 2018, p. 255 et s.

64. VERBRUGGEN, V., « Titre 1 - RGPD : coeur du puzzle de l'encadrement de la protection des données à caractère personnel dans l'Union Européenne », *Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Éditions Larcier, 2018, pp. 25 à 58.

65. VIEL, A., KINGSMILL, S. et MACLEOD, J., *Privacy for sale – To the highest bidder,* Deloitte report, 2017, disponible à l'adresse : « https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/deloitte-analytics/ca-en-data-ethics-and-privacy-survey.pdf », consulté le 16 avril 2019.

66. VINEZ, K., « The Admissibility of Data Collected from Wearable Devices », *Stetson Journal of Advocacy and the Law*, 2017, p. 10, disponible à l'adresse : « https://www2.stetson.edu/advocacy-journal/wp-content/uploads/2017/06/Vinez_-_Wearables.pdf », consulté le 9 avril 2019.

67. WOLF, G., *Our three prime questions*, Quantified self website, 2011, disponible sur : http://quantifiedself.com/2011/09/our-three-prime-questions/, consulté le 17 février 2019.

68. WOLF, G., « The data driven life », *The New York Times Magazine*, 2010, disponible en ligne à l'adresse : « https://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html », consulté le 20 mai 2019.

Jurisprudence

1. C.J.C.E., 6 novembre 2003, arrêt *Lindqvist*, C-101/01.

2. C.J.C.E., 16 décembre 2008, arrêt *Tietosuojavaltuutettu c. Satakunnan markkinapörssi oy et Satamedia o*y, C-73/07.

3. C.J.U.E., 1er octobre 2015, arrêt *Weltimmo s.r.o. contre Nemzeti Adatvédelmi és Információszabadság Hatóság,*, C-230/14.

4. C.J.U.E., 20 décembre 2017, arrêt *Novak*, C-434/16.

5. Cour Suprême autrichienne, 30 aout 2018, 6 Ob 140/18h, disponible à l'adresse : « https://www.lexfutura.ch/fileadmin/lexfutura.ch/Bilder/Blog/OGH_31.08.2018_6_Ob_140_18h.pdf », consulté le 19 avril 2019.

6. Cour suprême de Cassation italienne, 2 juillet 2018, n°17278/2018, disponible en ligne à l'adresse : « https://www.lexfutura.ch/fileadmin/lexfutura.ch/Bilder/Blog/_20180702_snciv%40s10%40a2018%40n17278%40tS.clean.pdf », consulté le 19 avril 2019.

7. Cass., 11 décembre 1970, *Arr. Cass.,* 1971, p. 369.

8. Cass., 9 février 1973, *Arr. Cass.,* 1973, p. 579 ; *Pas.*, 1973, I, p. 551 ; *R.C.J.B.*, 1974, p. 187, Note R. DE SMET.

9. Cass. 20 avril 2017, *DAOR*, 2017, p.54 ; *N.J.W.*, 2017, p.540, note P. BRULEZ.

10. Bruxelles, 23 mars 2012, *D.C.C.R.*, 2013/2, p. 49.

11. J.P. Zomergem, 11 mars 2011, *R.W.*, 2011-2012/30, p. 1347.

Législation

Législation Européenne

1. Proposition amendée pour une directive du Conseil sur la protection des individus au regard du traitement de données personnelles et à la libre circulation de ces données, *COM(92) 422 final - SYN 287*, 28 octobre 1992.

2. Position commune (CE) relative à l'adoption de la directive 95/46/CE en vue de l'adoption de la directive 95/46/CE du parlement et du conseil, du 24 octobre 1995, relative à la protection des données à caractère personnel et à la libre circulation de ces données*, J.O.C.E* 13 avril 1995*,* p. 20.

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

4. 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.*, L119 du 4 mai 2016, pp. 1 à 88.

Législation Belge

1. Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 février 1993.

2. Loi du 4 avril 2014 relative aux assurances, *M.B.*, 30 avril 2014, article 58.

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

Annexe : Interview Laurent Baijot : CEO ForMyFit

Monsieur Laurent BAIJOT est le co-fondateur de l'entreprise et de l'application homonyme, *Formyfit*.

Tout d'abord, une première prise de contact et explication du contexte de mon mémoire à Monsieur BAIJOT: Explication de la question de recherche, de la dynamique dans laquelle s'inscrit le travail et du choix d'une entreprise telle que *Formyfit* pour tenir cette interview,…

Q1 : Comment est née cette idée de développer une application sportive telle que Formyfit, c'est à dire une application de course à pied avec un coach intégré ?

L'idée de départ c'est, que Monsieur BAIJOT vient d'un village assez reculé dans les Ardennes. Il a commencé le sport tard, vers 12 ans, il a gagné le cross de son école, puis le francophone, puis les championnats d'Europe,… Il était assez fort, après un an ou deux, un club d'athlétisme est venu le chercher, il n'est pas tombé sur de bons entraineurs, il a continué à progresser car, selon lui, il a une bonne génétique lui permettant de progresser. Il n'a pour autant pas pu progresser comme il aurait pu le faire s'il avait rencontré le bon coach dès le départ. Il a tout de même réalisé l'école militaire ne tant qu'officier car, au début des années 90, tous les athlètes étaient militaires. Ne s'y plaisant pas, il a bifurqué vers une licence en éducation physique à l'UCL en étant étudiant chercheur en physiologie de l'effort, collaboré avec le labo de physiologie avec lequel son entreprise continue de collaborer. Malgré cela, pendant 10 ans, il estime s'être entrainé trop dur, n'a plus progressé, ce qui a entrainé de nombreuses frustrations malgré son très bon niveau (10 meilleurs belges).

Ensuite, il a découvert un coach vers ses 35 ans qui l'a fait retravailler la base avec une méthode d'entrainement conforme à la littérature scientifique. L'idée est donc de progresser plus en produisant un effort moins intense, et par conséquent, il serait dommage de ne pas en faire profiter plus que les gens qui pouvaient rencontrer ce coach. L'idée était donc de généraliser la méthode, tant pout Monsieur BAIJOT, tant que pour le coach en question. De l'idée à l'implémentation, il a fallu trouver du financement, des partenaires,…

Monsieur Baijot a également longtemps travaillé dans le domaine du pharmaceutique, avec parcours assez ascendant, il est passé par délégué médical, hospitalier, directeur d'équipe, directeur des ventes, directeur marketing, management team,… en passant par quatre grands groupes dans un desquels il a décroché un poste au sein du comité de direction. Dans ces entreprises il a développé

un outil permettant au médecin généraliste d'identifier quels étaient ses patients avec le plus haut risque cardio-vasculaire. Dès lors le médecin pouvait mettre en place un traitement adéquat et proactif sur basé la prévention et le traitement médicamenteux. On s'est ensuite rendu compte que l'activité physique avait un impact plus grand que les médicaments dans la prévention cardio-vasculaire, du diabète, de pathologies chroniques et également le cancer.

Assez rapidement est venue l'idée de faire une application qui concernait non seulement le sport mais aussi ayant pour but de faire bouger les gens. L'application n'a pas encore atteint cet objectif, ce sera, selon lui, plus compliqué parce que cela implique des données médicales en non sportives. Selon qu'il discute avec l'une ou l'autre personne, certaines considèrent les données telles que la fréquence cardiaque comme sensibles alors que d'autres non.

Q2 : En ce qui concerne le modèle économique de ce type d'applications, comment vous est il venue l'idée de partir sur un modèle payant alors que les autres applications utilisent un modèle Freemium ?

Pour Monsieur BAIJOT, cette question symbolise parfaitement leur mauvaise communication à cet égard : il existe bien une version gratuite de l'application qui permette faire du tracking, de mesurer, d'historiser, et de faire tout comme une autre application. Il n'y a dès lors que la dimension plan d'entraînement qui est payante, comme chez les autres.

Au niveau des contrats qu'ils développent, ils ont d'abord estimé qu'un modèle exclusivement B2C était envisageable avec des campagnes Facebook, un taux de conversion suffisant vers le payant, de s'étendre au niveau mondial et que tout allait rouler comme cela.

Il n'en est rien, l'entreprise a du se diversifier pour passer également vers du B2B, trop tard selon Monsieur BAIJOT pour deux raisons : c'est un canal de diffusion beaucoup plus simple, pas besoin de faire des campagnes pour toucher des gens, il suffit de contacter la personne en charge dans l'entreprise et ils payent *Formyfit* pour accéder à l'application. Ils reçoivent donc de l'argent pour que les employés utilisent l'application, les utilisateurs aiment l'application et parrainent leurs amis, … Ce modèle a permis en quelque sorte de sauver l'entreprise, en empêchant une nouvelle dilution du capital.

Q3 : Au commencement, quand vous avez pris connaissance avec la matière de la protection des données à caractère personnel comme l'avez vous perçue ? Plus comme une frein à l'innovation ou plus comme une nécessité afin de protéger des droits fondamentaux ?

Avant le GDPR, l'entreprise a mis un point d'honneur à essayer d'être le plus puissant possible par rapport à la protection des données individuelles et des serveurs. Ils se sont entourés dès le début par le Microsoft Innovation Center de Mons (MIC). Les développeurs ont d'abord été engagés comme étudiants, après qu'ils aient fait leur stage au MIC, les deux meilleurs sont restés et sont devenus salariés. Ce sont les mêmes développeurs depuis le début dans l'entreprise. Ils ont eu la volonté d'être le plus *safe* possible quant à ces données. Tout est stocké sur un serveur qui est chez Azure[252], donc stocké en Europe, ce qui écarte toutes les règles concernant le transfert de données vers des pays tiers à l'Union Européenne. De plus, la majorité des utilisateurs se trouvent en Europe « francophone », c'est à dire France, Suisse et Belgique.

Intervention personnelle : C'est en quelque sorte une expression du *Privacy by Design*, à la base tout est fait pour être le plus *compliant* possible avec la matière du RGPD. Plutôt que de développer et puis de chercher comment protéger les données, dès la conception du produit, vous vous êtes orientés vers une politique de protection et avoir une base saine.

Une chose importante est que seulement deux personnes au sein de l'entreprise ont accès aux données, ces données ne sont consultées que sur demande des utilisateurs. Par exemple, un cas pratique qui s'est déroulé il y a très peu de temps : lors de l'*Urban Trail de Tournai*, le parcours fait 10km, un utilisateur contacte l'entreprise parce que l'application affiche 18km alors que son traqueur affiche la bonne distance. *Formyfit* envoie alors un mail pour demander l'accord de l'utilisateur pour aller dans la base de données afin de comprendre ce qui s'est passé. Pour les utilisateurs qui fonctionnent sous Android, ils ont mis en place un filtre de Kalman[253] qui corrige les erreurs de tracé, par contre sur iOS, ils n'ont pas jugé nécessaire de le mettre en place. Il est arrivé que cet *Urban Trail* passe au travers du cinéma, des monuments historiques,… ce qui amène parfois le GPS à aller rechercher un point très éloigné de l'endroit où se trouve l'appareil à cause de la

[252] https://azure.microsoft.com/fr-fr/

[253] Le filtre de Kalman est un algorithme qui permet d'estimer l'état d'un système à partir des données mesurées. Dans les applications de vision par ordinateur, les filtres de Kalman sont utilisés pour le suivi d'objets afin de prédire la future position d'un objet, de prendre en compte le bruit associé à la détection et de permettre d'associer plusieurs objets à leurs pistes correspondantes. Filtre de Kalman, article en ligne, disponible à l'adresse : « https://fr.mathworks.com/discovery/kalman-filter.html », consulté le 30 avril 2019.

mauvaise connexion. C'est ce qui s'est passé dans ce cas-ci. Ils ont donc demandé à l'utilisateur pour aller voir dans ses données.

Relance de la question: ce type de législation vous retient il dans le développement de votre business ?

Monsieur BAIJOT explique que ce type de législation leur a fait très peur, comme à tout le monde et puis plus l'on en parlait plus cela faisait peur. Lorsqu'il est sorti, Monsieur BAIJOT était en formation *MedTech*, ces centres dispersés à travers la Belgique se sont réunis pour proposer une formation GDPR spécialisée dans ce domaine. La formation était de 18 journées (ce qui est conséquent), ils ont reçu des cours sur ce sujet. Selon lui, le GDPR a aussi un peu perdu de vue l'objectif de protéger les petites entreprises contre les géants du net. Il estime également qu'il a moins de soucis à se faire car les autorités vont d'abord s'intéresser à ce qui se passe chez les grands que de venir chez eux. Chez eux, ils mettent tout en place pour être le plus sur possible de ne pas avoir de problèmes le jour où un contrôle devait arriver.

La problématique globale est qu'il est nécessaire d'être blindé sur les plans d'entrainement, sur le GDPR, et dans plein de domaines… C'est donc super d'être une entreprise comme Runtastic où il y a 300 personnes qui y travaillent non stop sur le marketing, le développement,… chez *Formyfit*, ils ne sont que 4 et c'est délicat de tout gérer.

Q4. Selon vous, est ce que le retrait du consentement est une notion qui pose des problèmes en pratique ?

Le retrait du consentement n'est pas quelque chose d'exorbitant selon lui, il n'existe que très peu de demandes et de par leur organisation concernant les données, cela reste assez simple. Selon lui, on en fait toute une montagne mais c'est relativement simple, ils n'ont eu que deux demandes.

Ecart pratique sur un cas de figure récurrent : Ce sur quoi ils ont le plus de demandes concerne plus la suppression de comptes qui sont faits en doublon par les personnes plus âgées qui ont plus de mal avec les adresses électroniques. Ils s'enregistrent avec une adresse mail puis avec une autre parce qu'ils pensent que la première ne fonctionne plus alors qu'ils ont juste rajouté un caractère supplémentaires, et viennent ensuite se plaindre que leur compte n'a plus leurs données ou qu'ils n'arrivent plus à avoir accès à leur compte. Il faut donc encore demander l'accord pour aller dans la base de données.

Là où il y a plus de demandes, c'est en ce qui concerne les e-mails automatiques. Il existe un tunnel d'e-mails en fonction de l'avancement de l'utilisateur dans l'application, via MailChimp. Il y a des gens qui se désinscrivent, c'est généralement 2 à 3 par semaine.

Q5. En ce qui concerne les méthodes de légitimation du traitement des données, il existe celle du consentement au traitement des données. Lorsque le consentement est requis, comment recueillez vous ce consentement ?

L'application fonctionne en deux temps, d'abord il y a une acceptation globale de la politique de vie privée lorsque l'on s'inscrit. Ensuite, il y a des pop-ups spécifiques pour les traitements de données comme le GPS, l'accès à l'application « Santé » sur iOS pour récupérer le nombre de pas, ou GoogleFit pour Android,… De plus, si les personnes ne font rien le traitement de données ne sera pas autorisé par l'application. Il y a donc souvent des utilisateurs qui viennent demander pourquoi leur séance n'a pas été enregistrée, la cause se trouve souvent dans le fait qu'ils n'ont pas accepté le pop-up.

Intervention personnelle : Ce système de pop-ups est intéressant car dans les hypothèses où l'on va récupérer des données de santé, on tombe dans le traitement de données sensibles. Pour que ce traitement puisse se faire, il est requis par le RGPD d'avoir un consentement spécifique au traitement de ces données. Dès lors, les pop-ups peuvent être vus comme une façon adéquate de recueillir le consentement spécifique requis dans le cadre du traitement de données sensibles.

C'était une recommandation qui avait été faite lors de la formation MedTech que Monsieur BAIJOT a suivie. Lorsque l'on télécharge l'application il n'y a que très peu de personnes qui lisent la politique de confidentialité.

Q6. Pour enchainer sur cette problématique, pensez-vous qu'une personne quand elle arrive sur une application comme la votre, qu'elle a cette politique de confidentialité devant elle et qu'elle ne lira certainement pas, peut on considérer qu'elle donne réellement son consentement au traitement de ces données ? Ce moyen de légitimer le traitement des données n'est il dès lors pas fragile ?

C'est sûr, Monsieur BAIJOT estime que c'est quelque chose qui protège l'entreprise plus que la personne concernée. Il veut télécharger l'application et il doit accepter, soit il lit tout, il se peut dès lors qu'il y ait des points qui lui déplaisent mais dans tous les cas, il n'aura pas le choix s'il veut utiliser l'application. Chez *Formyfit*, la personne concernée accepte dans un premier temps la base

qui permet à l'application de fonctionner. Ensuite il ya des pop-ups qui viendront ensuite pour légitimer certains traitements. De base, ils ne se connectent pas au GPS, à l'application « Santé », à sa connexion avec sa ceinture,… D'ailleurs, l'utilisateur doit à chaque fois réappuyer sur une certaine icône afin de relancer la connexion entre l'application et son traqueur. La personne doit alors faire la démarche activement.

Q7. La démarche de mon mémoire a pour but d'aller plus loin que de juste déclarer que les personnes concernées ne sont pas capables de consentir au traitement de leurs données. Dès lors, j'ai repris l'idée de promouvoir des icônes (telles que celles de Privacy Tech) que l'on pourrait mettre au sein des applications et sur les sites internets afin que la personne concernée puisse facilement se rendre compte du traitement des données. Qu'en pensez vous ?

Cela pourrait notamment se trouver au sein des paramètres avec en dessous, les icônes les plus importantes comme par exemple la collecte de données sensibles sur la santé représentées par un coeur. L'utilisateur pourrait dès lors appuyer dessus pour avoir un détail des données de santé collectées. Monsieur BAIJOT trouve que ce serait une bonne idée et qu'une telle fragmentation de la politique de vie privée pourrait être bénéfique à la compréhension globale. Il émet également l'idée que l'on puisse directement, au travers de cette icône, accéder aux paramètres de confidentialité concernant le traitement de ces données là.

Q8. Notre discussion dévie sur la question des classements au sein des applications de quantified self

Au sein de l'application, il existe un classement « FIT », il est divisé en un classement général et un classement mensuel, ce sont des points attribués par l'application aux utilisateurs afin d'établir leur position par rapport aux autres et d'obtenir un certain rang dans l'application. (Renvoi à la gamification au sein des applications de quantified self). Au sein de ce classement, les noms des utilisateurs ne sont pas dévoilés s'ils ne le souhaitent pas, de plus, il n'existe pas de profil accessible par d'autres utilisateurs, la dimension réseau social n'étant pas encore développées (voir infra). C'est donc la volonté de la personne de dévoiler qui elle est au sien du classement « FIT ». L'application n'affiche que les 50 premiers.

Q9. Au sujet de la collaboration éventuelle entre un dispositif de quantified self et une compagnie d'assurance, que serait il possible de voir arriver sur le marché dans les prochaines années ?

Pendant une année, l'entreprise et une banque ont construit un *case* spécifique pour les assurances à partir de quelque chose d'assez basique au début. Par exemple pour les indépendants, ceux-ci souscrivent à une assurance revenu garanti dans le cas où ils tomberaient malade et ne pourraient plue exercer leur fonction pendant une période. C'est quelque chose qui coute relativement cher en fonction de ce que l'on demande comme revenu lors de cette période. Cette prime va dépendre majoritairement de malus comme le fait de fumer, le fait d'être en surpoids,… mais il n'y a pas de bonus. L'idée serait donc de donner un bonus plutôt qu'un malus comme il est fait avec les assurances RC auto. La compagnie d'assurances était assez enthousiaste par rapport à ce projet et Monsieur BAIJOT a été mis en contact avec le réassureur avec qui ils ont construit le *case*, en collaboration avec le légal et le scientifique.

L'idée était de se démarquer des compagnies qui sont déjà dans ce business telles que Vitality (Grande-Bretagne) et Oscar (États-Unis) qui se basent uniquement sur le comportemental pour faire varier les primes d'assurance.

Q10. La discussion dévie sur la question de la triche au sein des applications de quantified self

Il y a énormément de tricheurs pour l'instant. Au sein de l'application, les FITS ne rapportent presque rien pour l'instant, seulement des abonnements pour les meilleurs ainsi que quelques places pour aller voir des matchs de football. A l'avenir, l'entreprise va peut être signer un contrat avec « *Running Warehouse* », pour, en fonction du niveau de la personne dans l'application, lui offrir des réductions sur des articles de sport.

Monsieur BAIJOT explique comment fonctionne le cumul de points sur l'application, qui pourront potentiellement à l'avenir donner des réductions. Si l'on enclenche un mode « course » on obtient 300 FITS, un mode « entrainement » 100 FITS plus les calories et un mode « *freerun* » 1 minute/fit avec une limite de 50. Certaines personnes ne faisaient que des mode « course » afin d'obtenir le plus de points possible, certains se plaignaient d'ailleurs car ils ne recevaient parfois pas leurs points. Ces personnes ont donc contacté l'application qui leur a demandé leur consentement pour aller au sein de la base de données, et *Formyfit* a découvert qu'il ne faisait que des modes course afin d'obtenir le plus de points possible à chaque fois. De nombreuses balises ont été mises en place

: en ce qui concerne le mode course, les deux premières sur le mois vont rapporter 300FITS chacune, les suivantes ne rapporteront plus rien. Même chose en ce qui concerne le mode Freerun, certains lançaient l'application en laissant tourner alors qu'ils ne réalisaient aucun exercice, juste pour obtenir les points. Il y a donc désormais un minimum de 4 km/h en course et 8km/h en vélo pour obtenir les points.

Il y a également des gens qui courraient avec deux téléphones pour avoir deux fois les points, ou l'Apple Watch et le téléphone, dès lors si une course est lancée plusieurs fois depuis le même compte dans un laps de temps de cinq minutes, elle ne sera prise en compte qu'une fois.

Il y a donc des règles pour éviter les tricheurs mais il y en aura toujours, c'est en quelque sorte la nature humaine.

Q11. Plusieurs applications fonctionnent avec un réseau social directement dans l'application, est ce un choix délibéré de ne pas avoir mis un réseau social ou c'est quelque chose de trop compliqué ou qui n'a pas d'intérêt selon vous ?

C'est quelque chose que *Formyfit* souhaite développer, mais qui demande beaucoup de temps et qui ne va pas les différencier outre mesure de leurs concurrents. Il y a deux applications concurrentes basées sur du social comme Strava et Nike+, ils savent qu'ils doivent y arriver mais c'est quelque chose qui demande beaucoup d'efforts et ce n'est pas la priorité en ce moment.

Par contre, ils ont une page Facebook et un groupe Facebook « Formyfit-communauté ». Sur le groupe, ce sont surtout les utilisateurs qui ont mis cela en place, ils discutent entre eux, ils se donnent des rendez-vous,… L'entreprise essaye de ne pas trop intervenir et laisser la communauté faire, Monsieur BAIJOT va souvent voir, répond à certaines questions et valide certaines réponses.

Q12. Comment l'application fonctionne t'elle en collaboration avec le traqueur ?

Tous les traqueurs ne sont pas compatibles avec l'application *Formyfit*, ils sont les seuls sur l'Apple Watch à faire du coaching, ce qui est étonnant mais compréhensible car c'est très difficile à développer. Une des raisons est que le logiciel de l'apple watch a beaucoup de limitations, il y a de nombreux crashs, c'est assez peu fiable au niveau de la fréquence cardiaque avant le 3eme génération. C'est d'ailleurs parfois gênant car c'est sur cette base que l'on calcule les plans d'entrainement et cela donne donc des plans inadaptés car la mesure de base n'est pas juste. Ils sont

donc tributaires de la technologie offerte par les constructeurs. Cela évolue tellement vite que c'est plus simple d'être sur du logiciel plutôt que sur de la technologie physique qui est rapidement obsolète.

Q12. Comment fonctionne la modification d'une politique de confidentialité ? Est ce que la détermination de la finalité du traitement a priori est un obstacle au développement futur de l'application ?

Il est nécessaire de publier une nouvelle mise à jour de l'application et à ce moment là, il est également nécessaire de ré-accepter la politique de l'application. Par exemple, récemment, ils ont rajouté un partenaire dans l'application qui est un magasine de course à pied. Il est faut alors coder cela dans l'application, qu'Apple valide la modification de l'application et s'ils acceptent, ils publient dans les trois jours.

Q13. Discussion sur Formyfit en général, sa vision et sa mission

Leur but général c'est d'améliorer la santé des gens par la pratique de l'activité physique, tout revient toujours à ça. Cela passe notamment par une pratique régulière de l'activité physique, encadrée, via des méthodes assez douces qui permettent de progresser. C'est un peu l'inverse des autres applications qui poussent chaque fois à aller plus loin et même parfois trop loin. Selon Monsieur BAIJOT, le message est parfois difficile à faire passer, mais cela fonctionne bien en termes de marketing car ce type de message prône à se battre contre les concurrents qui se comportent de la mauvaise manière, en poussant les utilisateurs à aller trop loin, ce qui ne les aide pas à améliorer leur santé.

Q14. Discussion sur le futur de Formyfit

Ils sont partis d'abord vers l'utilisateur lambda sédentaire qui veut se bouger pour améliorer sa santé, perdre du poids,… Maintenant, ils s'orientent plus vers le patient diabétique en surpoids ou dans l'enseignement. Par exemple dans l'enseignement, on a des blocs d'endurance pendant 2 mois, ce n'est pas facile pour le professeur de faire quelque chose d'individualisé. En effet, les enfants n'ont pas tous eu une pratique sportive et tous les ados doivent réaliser le même parcours sans différenciation. Il faudra faire des études cliniques pour prouver que le niveau de santé va s'améliorer avec *Formyfit*, plutôt qu'avec l'enseignement classique. Ils font le test de VMA avec le professeur à l'école, comme ça il n'y aura pas de triche. Ils viennent avec un smartphone, ils font ce

test une fois par mois, et le reste du temps, ils demandent de courir, une, deux, trois fois semaine en « devoir pour le cours d'éducation physique » chez eux. Le professeur de gym a une interface qui lui permettrait de contrôler ce qu'il se passe, d'envoyer des notifications à ceux qui ne font rien ou à ceux qui font quelque chose. Ils vont pouvoir récolter des data et montrer qu'après un, deux ou trois mois, on a augmenté,… Ce sont peut être des projets à construire avec des mutuelles, le but est surtout de faire de la prévention, cela concerne aussi les petits.

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