Le mouvement “ Quantified Self ” et les données personnelles : étude de cas des applications mobiles de running

Maxime Arbonel

Vous allez consulter un mémoire réalisé par un étudiant dans le cadre de sa scolarité à Sciences Po Grenoble. L'établissement ne pourra être tenu pour responsable des propos contenus dans ce travail.

Afin de respecter la législation sur le droit d'auteur, ce mémoire est diffusé sur Internet en version protégée sans les annexes. La version intégrale est uniquement disponible en intranet.

SCIENCES PO GRENOBLE
1030 avenue Centrale – 38040 GRENOBLE
http://www.sciencespo-grenoble.fr

UNIVERSITÉ GRENOBLE ALPES

Institut d'études Politiques de Grenoble

Maxime ARBONEL

LE MOUVEMENT QUANTIFIED SELF ET LES DONNÉES PERSONNELLES : ÉTUDE DE CAS DES APPLICATIONS MOBILES DE RUNNING

Année 2015-2016

Master Transmedia

Sous la direction de Pascal Clouaire et Daniel Bouillot

UNIVERSITÉ GRENOBLE ALPES

Institut d'études Politiques de Grenoble

Maxime ARBONEL

LE MOUVEMENT QUANTIFIED SELF ET LES DONNÉES PERSONNELLES : ÉTUDE DE CAS DES APPLICATIONS MOBILES DE RUNNING

Année 2015-2016

Master Transmedia

Sous la direction de Pascal Clouaire et Daniel Bouillot

« De pair avec cet accroissement et ce perfectionnement de la puissance de la connaissance à l'égard de la totalité, l'homme acquiert sur le monde ambiant de sa *praxis* une domination toujours plus parfaite et qui s'étend en un progrès infini »[1]

[1] HUSSERL, Edmond. *La crise des sciences européennes et phénoménologie transcendantes*. 1976, p.76.

Remerciements

Je voudrais tout d'abord adresser mes remerciements aux deux directeurs du master Transmedia de l'IEP de Grenoble, Pascal Clouaire et Daniel Bouillot, qui ont contribué à faire de ce travail de recherche un moment de réflexion passionnant et enrichissant.

Je remercie également les personnes qui ont accepté de répondre à mes questions au cours des divers entretiens menés. Merci à Camille Charrier, Coralie César, Julie Chucherko, Julien Buecheler et Olivia Barrot qui m'ont incité à prendre du recul sur le sujet et y aborder les différents angles d'approches possibles. Je tenais également à remercier mes collègues de travail pour le temps passé à répondre à mes (nombreuses) interrogations et qui ont su m'apporter leur point de vue de façon claire et détaillée.

Enfin, je tenais à remercier ma famille et mes amis pour leur soutien et leur précieuse capacité d'écoute au cours de ces dernières années.

Sommaire

Introduction

Le 16 novembre 2015, l'institution américaine Federal Trade Commission (FTC) a organisé un workshop autour de la question du « *Cross-Device Tracking* »[2]. Dans un contexte de multiplication des appareils de lecture (ordinateurs portables, smartphones, tablettes…), les discussions ont porté sur les nouvelles technologies utilisées par les entreprises permettant de suivre les consommateurs et sur les enjeux soulevés du point de vue de la vie privée de ces derniers. En réponse à cet événement, le Center for Democracy & Technology (CDT) a publié un document le 16 octobre de la même année qui mettait en avant une technologie appelée « *SilverPush* »[3]. Développée par l'entreprise indienne SilverEdge, la technologie *SilverPush* permettait aux publicitaires de diffuser un signal ultrason appelé « *Sound beacon* », inaudible pour les utilisateurs, en même temps que la diffusion de publicités. Ce signal pouvait alors ensuite être capté par les applications ayant la logiciel SilverPush installé et ainsi être renvoyé à l'entreprise-mère. Grâce à ce processus technique, SilverEdge offrait la possibilité de connaître avec précision la localisation des spectateurs des publicités, la chaîne de télévision concernée, etc.[4]

Cette technologie a provoqué une levée de boucliers de la part de nombreuses institutions américaines et internationales du fait qu'elle permettait à l'entreprise-mère SilverEdge de récupérer un grand nombre de données personnelles des individus : le numéro d'identification de l'appareil, l'adresse MAC du routeur Wi-Fi, les caractéristiques du système d'exploitation mais aussi leur numéro de téléphone. Plus encore, cette captation des données personnelles se faisait à l'insu des individus, sans aucun consentement de leur part. Il était également impossible de refuser l'accès à ses données. Un autre problème souligné par ces institutions a été le transfert non sécurisé des données vers les serveurs de l'entreprise[5]. Sur son blog, le fournisseur d'antivirus Avira a mis en ligne un article intitulé « Avira now identifies SilverPush ad-tracking as malware » en fin d'année 2015. Le PDG d'Avira y

[2] https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking
[3] CALABRESE, Chris, MCINNIS, Katherine L., HANS, G.S. et NORCIE, Greg, "Comments for November 2015 Workshop on Cross-Device Tracking, https://cdt.org/files/2015/10/10.16.15-CDT-Cross-Device-Comments.pdf, consulté le 08/03/16.
[4] Voir Annexe 1
[5] THOMSON, Iain, « How TV ads silently ping commands to phones: Sneaky SilverPush code reverse-Engineered", http://www.theregister.co.uk/2015/11/20/silverpush_soundwave_ad_tracker/, consulté le 09/03/16.

affirmait les éléments suivants : « *The functionality of the SilverPush software is way out of line for a legitimate advertising software development kit – given the way this software sucks up data on the individual user, the extend of this data, and the insecure transport of this data back to SilverPush – so we are now be detecting this as a Trojan* ».[6]

Au vu des éléments précédents, la technologie utilisée par SilverEdge soulève d'importantes questions concernant le respect de la vie privée des individus. Selon le document de réponse du Center of Democracy & Technology à la Federal Trade Commission, le constat fut le suivant :

> This level of detailed and pervasive surveillance creates obvious privacy issues. At a basic level it is very difficult for a user to make sensitive purchases without companies logging and tracking this activity. Further, when a company combines the information from the different devices, an extremely detailed picture emerges. […] *The combination of information across devices not only creates serious privacy concerns, but also allows companies to make incorrect and possibly harmful assumptions about individuals*.

Véritable point de départ de notre réflexion, le cas de la technologie SilverPush reflète les enjeux que représentent les avancées technologiques du point de vue de l'utilisation des données personnelles et de la vie privée des individus, tant en ligne que hors ligne. Ces dernières années, l'actualité internationale a été marquée par de nombreux faits mettant en avant les pratiques, souvent opaques, de grandes firmes et organisations concernant les données personnelles des individus. Il est possible d'évoquer les révélations successives de l'ancien agent de l'agence américaine NSA Edward Snowden à partir du 6 juin 2013 ou encore les contestations autour du projet de « Privacy Shield ». Ces différents faits d'actualité, et les polémiques qui en découlèrent, s'implantent au sein de tendances qu'il est nécessaire de rappeler avant toute analyse plus approfondie.

Tout d'abord, on a pu assister à l'émergence croissante du web mobile et des usages permis par ce dernier. En effet, le smartphone, ou « téléphone intelligent », s'est récemment imposé en devenant le premier appareil permettant la consultation web. Selon Canalys, plus d'1.5 milliards de smartphones seront vendus dans le monde à la fin de l'année 2016[7]. Plus encore, selon le rapport « Cisco Visual Networking Index : Global Mobile Data Traffic

[6] FRINK, Lyle, "Avira now identifies SilverPush ad-tracking as malware", http://blog.avira.com/silverpush-malware/, consulté le 07/03/16.

[7] « Media Alert: Over 1.5 billion smart phones to ship worldwide in 2016", Canalys, http://www.canalys.com/newsroom/media-alert-over-15-billion-smart-phones-ship-worldwide-2016, consulté le 12/03/16.

Forecast Update 2015-2020 », le trafic des données mobiles s'est accru de 74% en 2015, atteignant plus de 3,7 exabytes par mois à la fin de l'année 2015 (contre 2,1 exabytes en 2014). Ce même rapport estime que la masse des données mobiles représentera 30,6 exabytes en 2020 et que le nombre total de smartphones atteindra plus de 50% de l'ensemble des appareils et des connexions au cours de la même année[8]. Au-delà de ces données statistiques, il est possible de souligner un tournant majeur : celui du passage de l'ordinateur au mobile. Sans pour autant remplacer le premier, le second s'est imposé comme un *device* populaire en raison de sa mobilité et des différentes applications qu'il est possible d'installer en son sein. Ces précédentes caractéristiques ont mené à l'essor de nouvelles pratiques mais aussi à de nouvelles relations entre les individus et la sphère numérique. Cette mobilité des usages a été un vecteur de changement tant pour les organisations que pour les individus.

Ensuite, autre tendance majeure, le concept de « *Big Data* » s'est rapidement popularisé pour qualifier l'explosion des données à l'échelle mondiale. Un travail important de définitions a pu être accompli à partir de 2001. Pour une pluralité d'auteurs, l'expression « Big Data » permet d'illustrer une explosion des données selon les fameux « *three Vs* ». Pour Doug Laney, analyste à Gartner (anciennement META Group), dans son article « 3D Management: Controlling Data Volume, Velocity and Variety » [9], la gestion des données de masse avait trois caractéristiques : le volume, la variété et la vitesse.[10] Cette typologie fut ensuite reprise pour définir ce « Big Data », popularisée notamment par le numéro de la revue Nature datant de 2008 et intitulé « Big data: science in the petabyte era »[11]. Selon Pierre Delort, dans son ouvrage *Le Big Data*, « le Big Data consiste à créer en exploratoire et *par induction* sur des masses de données *à faible densité* en information des modèles *à capacité prédictive* »[12]. Cette définition permet de mettre en évidence trois autres caractéristiques du Big Data : un raisonnement inductif, un grand volume de données à faible densité et des modèles prédictifs. Eric Sadin, écrivain et philosophe parle quant à lui d'une « datification » du monde, qu'il définit de la manière suivante :

[8] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015-2020 White Paper, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html, consulté le 12/03/16.
[9] LANEY, Doug, "3D Data Management: Controlling Data Volume, Velocity and Variety", 6 February 2001.
[10] Voir Annexe 2
[11] Nature, International weekly journal of science, « Big data: science in the petabyte era", Editor's summary, 4 September 2008, http://www.nature.com/nature/journal/v455/n7209/edsumm/e080904-01.html, consulté le 20/04/16.
[12] DELORT, Pierre, *Le Big Data*, Presses Universitaires de France, 2015.

> Désormais, chaque événement est peut être capté en tant que tel et témoigner de sa qualité propre, autant qu'être virtuellement être mis en lien avec tout autre. C'est cela la mise en donnée du monde, sa datafication, ne s'éprouvant plus comme un horizon infini de faits épars, mais comme un *registre intarissable d'équations évolutives, exposant ou révélant en temps réel l'état général et singulier des choses grâce à la réduction numérique universelle* relayée par la puissance des systèmes corrélatifs et d'algorithmes interprétatifs.[13][14]

Pour Simon Chignard et Louis-David Benyayer, trois transformations majeures ont été engendrées par un monde de données abondantes : un changement de la nature même des données qui peuvent être mobilisées, un changement de la valeur, passant de la rareté à l'abondance et, enfin, l'émergence d'une économie de la donnée selon trois facettes (la matière première, le levier et l'actif stratégique).[15] Ainsi, et nous y reviendrons tout au long de ce mémoire, le Big Data a permis le développement de nouvelles pratiques des entreprises, allant de la captation à la revente des données personnelles des utilisateurs en passant par leur traitement et leur analyse. Ces usages de la donnée ont pu être vus par certaines institutions et certains acteurs comme de profondes atteintes à la vie privée des utilisateurs.

Enfin, la troisième et dernière tendance à prendre en compte est celle du « Quantified Self ». Selon Camille Gicquel et Pierre Guyot, le « Quantified Self » peut être défini comme « un ensemble de méthodes visant à collecter et utiliser soi-même certaines variables concernant son propre corps et ses propres comportements »[16]. D'autres éléments de définition ont pu été apportés par Melanie Swan en 2013[17] :

> The Quantified Self is any individual engaged in the self-tracking of any kind of biological, physical, behavorial or environmental information. There is a proactive stance towards obtaining information and acting on it. A variety of areas may be tracked and analyzed, for example weight, energy level, mood, time usage, sleep quality health cognitive performance, athletics and learning strategies.[18]

[13] SADIN, Eric, *La vie algorithmique, critique de la raison numérique*, éditions L'échappée, 2015.
[14] Voir Annexe 3
[15] CHIGNARD, Simon et BENYAYER, Louis-David, *Datanomics, les nouveaux business models des données*, Editions FYP, 2015.
[16] GICQUEL, Camille et GUYOT, Pierre, *Quantified Self, les apprentis sorciers du « moi connecté », Editions FYP, 2015.*
[17] SWAN, Melanie, "The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery", June 2013.
[18] Voir Annexe 4

Phénomène ancien ne datant pas de l'ère numérique, ce mouvement a été lancé par deux journalistes du magazine américain Wired, Kevin Kelly et Gary Wolf. Le slogan qui a pu être diffusé était : « la connaissance de soi par les nombres ». Derrière cette formule attractive, le « Quantified self » dépasse la simple auto-mesure de soi. En effet, il concoure à « la création d'un nouveau média dont la matière première est la donnée, collectée, analysée, croisée, exploitée »[19]. Ici encore, plusieurs enjeux peuvent être mis en avant concernant tant la perception des individus d'eux-mêmes que de la perception des autres par rapport à soi.

L'ensemble de ces tendances ont conduit à l'émergence de problématiques concernant la protection de la vie privée des utilisateurs. Avec SilverPush, un exemple parmi tant d'autres, il a pu être démontré qu'un nombre croissant de données personnelles des individus étaient et sont collectées par leurs smartphones et potentiellement utilisées par des acteurs tiers. Véritable terrain d'étude de ce travail, il est nécessaire d'analyser plus en avant les tenants et les aboutissements de ces pratiques à l'intersection des tendances précédemment mises en avant. Plus précisement, nous nous intérresserons aux applications mobiles téléchargeables gratuitement. En effet, ces dernières années, il a pu être constaté un essor de services accessibles gratuitement et fournis par des entreprises. Derrière cette gratuité, il est vrai que l'utilisateur final n'aura pas à payer le service en monnaie sonnante et trébuchante. Néanmoins, ces entreprises financent leurs activités par d'autres moyens, parfois méconnus du grand public et de leurs utilisateurs. D'une part, ce financement est possible grâce à des publicités soumises aux consommateurs. En échange de son "temps d'attention disponible", l'utilisateur peut accéder aux services concernés. D'autre part, et c'est l'objet de ce mémoire, les entreprises ont la possibilité de capter les données personnelles de leurs utilisateurs afin de les revendre à des acteurs tiers. Ces pratiques, que nous développerons plus loin, ne datent pas du web mobile mais ont d'ores et déjà pu atteindre un certain seuil de maturité sur le web. Malgré un changement de *devices*, le principe de captation des données personnelles repose fondamentalement sur le même processus. C'est dans ce cadre que des *business models*, ou modèles d'affaires, ont émergé qui reposent sur la captation, le traitement, l'échange ou la revente de ces données personnelles. L'objectif affiché est d'atteindre le seuil de rentabilité voire celui de profitabilité.

[19] GICQUEL, Camille et GUYOT, Pierre, *Quantified Self, les apprentis sorciers du « moi connecté », Editions FYP, 2015.*

Sur un grand nombre d'applications mobiles pouvant être téléchargées gratuitement *via* les principaux App Stores (l'Apple Store ou le Play Store par exemple), notre analyse portera plus précisement sur les applications mobiles développées dans la lignée du mouvement Quantified Self. En effet, outre par le biais d'objets connectés (dont le fameux bracelet FitBit), les applications mobiles ont permis d'user de toutes les possibilités offertes par les capteurs intégrés aux smartphones. Reliés à Internet en 4G ou en Wi-Fi, ces derniers sont devenus des outils de mesure mobiles et flexibles pour les utilisateurs pouvant servir à l'auto-captation de données. Dans ce cadre, nous étudierons un genre précis d'applications : les applications de santé et de bien-être (ou "*Health and wellness*" en anglais). Au sein de cette catégorie, notre étude portera sur les applications mobiles de course à pied. MapMyRun, Nike+ Running, Runstatic, Runkeeper, Strava... il existe une grande pluralité de ce type d'applications. Elles comptent également un très grand nombre d'utilisateurs à travers le monde. L'un des facteurs de ce succès repose notamment sur un téléchargement gratuit et une facilité d'utilisation.

Avec un cadre d'analyse précédemment défini, ce mémoire vise ainsi à étudier l'usage de ces applications mobiles par les individus en dépit de l'utilisation qui est faite de leurs données personnelles. Nous chercherons notamment à répondre à la question suivante : comment et pourquoi les utilisateurs choisissent-ils de céder une partie de leurs données personnelles et, ainsi, de dévoiler une partie de leur vie privée à des fournisseurs de services ? Plus encore, et ce sera le fil rouge de ce travail, en quoi le partage des mobinautes d'une partie de leurs données personnelles dans le but d'accéder à des applications en apparence gratuites met-il en lumière tant des logiques de perception et de processus de décision divergentes que d'une relation fondamentalement asymétrique entre les entreprises et les individus ?

Comme point de départ de cette réflexion, notre hypothèse de travail a été que, par souci de facilité et de rapidité, les individus sont prêts à céder une partie de leurs données personnelles à des entreprises afin d'accéder à des services divers. Ces démarches sont faites en opposition totale avec leurs discours, reflétant une certaine crainte vis-à-vis de la divulgation d'un pan conséquent de leur vie privée. Afin de vérifier cette hypothèse, notre travail se situera à la croisée des sciences de l'information et de la communication, de l'économie comportementale, de la sociologie et de la psychologie sociale. Avec cette hypothèse posée, il est nécessaire d'identifier préalablement trois types d'acteurs : les entreprises qui développent les applications mobiles, les utilisateurs de ces applications

mobiles et les sociétés tierces, appelées « *data brokers* ». Par souci de temps, ce mémoire va s'intéresser principalement aux seconds et à leurs rapports qu'ils entretiennent avec les premiers.

L'étude d'une partie du mouvement Quantified Self et de l'utilisation des données personnelles des utilisateurs représente une thématique large qu'il sera bien entendu impossible de traiter dans son intégralité. En cela, certaines questions ne seront volontairement pas traitées ici. Nous pouvons citer le cas des questions couvrant la sécurité informatique ou encore les questions d'ordre purement juridique. Comme énoncé précédemment, le Quantified Self englobe un grand nombre de pratiques. Ce travail ne traitera donc pas non plus des applications médicales mais aussi du champ des *wearables technologies*, c'est-à-dire de ces objets connectés permettant le recueil de données personnelles. Enfin, nous n'aborderons pas la question du partage volontaire des données personnelles par les utilisateurs, notamment sur les réseaux sociaux. De nombreuses études ont d'ores et déjà été publiées sur le sujet.

Afin de répondre aux interrogations précédentes, nous nous attacherons, dans un premier temps, à aborder la question du développement d'une offre pléthorique d'applications mobiles de running gratuites comme le reflet du développement des modèles d'affaires reposant sur les données personnelles pour ensuite analyser le décalage entre la perception et le processus décisionnel de leurs utilisateurs concernant la divulgation de leur vie privée. Enfin, cette réflexion nous conduira à explorer la nouvelle place des individus au sein de ce mouvement Quantified Self et y aborder les initiatives alternatives visant à protéger la vie privée des individus.

Outre la consultation de nombreux travaux sur les questions de données personnelles et de vie privée, l'un des autres piliers de ce travail a été l'organisation de plusieurs entretiens qualitatifs[20]. Suivant la méthodologie des sciences sociales, ces entretiens semi-directifs ont permis de mettre en lumière un second discours, différent du discours scientifique, c'est-à-dire celui des principaux concernés : les individus. Dans un contexte d'accélération des flux d'informations et de l'émergence de nouvelles technologies, la parole des individus a été essentielle à prendre en compte et a permis, *in fine*, de confirmer ou d'infirmer les conclusions des différents travaux scientifiques sur le sujet.

[20] Voir Annexe 8

Partie I : L'essor d'une offre pléthorique d'applications mobiles de running gratuites comme le reflet du développement de modèles d'affaires reposant sur les données personnelles

« Footing », « jogging », « running »… quelque soit l'expression utilisée, la course à pied a connu une progression importante de son nombre de pratiquants au cours de ces dernières années. Selon l'étude commandée par la Fédération Française d'Athlétisme à l'agence SportlabGroup et intitulée « Attitudes et comportements de pratique de course à pied », on dénombrait 9,5 millions de pratiquants (soit 20% des Français) en 2014. Parmi ces pratiques, cette même étude mettait en avant une forte diversité d'individus : 53% de femmes contre 47% d'hommes par exemple. En termes de pratiques, le « running » se pratique le plus généralement seul (pour 77% des pratiquants running) avec deux motivations principales : une bonne santé et une amélioration de sa condition physique.[21]

C'est dans ce contexte qu'on a pu assister au développement d'un nombre croissant d'applications mobiles visant spécifiquement ce type d'utilisateurs. Accessibles gratuitement tout en offrant parfois une version « *premium* », ces applications mobiles s'intègrent au mouvement Quantified Self, défini précédemment. Leur utilisation massive reflète un besoin de s'auto-mesurer afin d'améliorer sa condition physique de façon autonome. Au-delà d'une augmentation de l'offre, on constate également un intérêt croissant des marques de sport pour ce secteur en plein essor. Dernière illustration en date, le rachat de l'application Runkeeper par l'équipementier sportif Asics a été scellé à hauteur de 85 millions de dollars[22]. Autre exemple récent, on peut aussi noter le rachat de Runstatic par Adidas pour 220 millions de dollars. Outre un positionnement nécessaire face à des acteurs concurrents (par exemple Nike+ devenu Nike Running), les décisions de ces rachats reposent en partie sur les bases de données de ces organisations, composées essentiellement des données personnelles recueillies par ces applications. Après avoir effectué un travail de définition des termes fondamentaux de

[21] « Attitudes et comportements de pratiques du coureur à pied », Fédération Française d'Athlétisme et Sportlab, http://www.sporsora.com/ressources/etude-1/-1/449-scap-etude-1/file, consulté le 15/04/16.
[22] MATTEI, Alain, « L'application Runkeeper rachetée par Asics pour 85 millions de dollars, http://www.eurosport.fr/economie/l-application-runkeeper-rachetee-par-asics-pour-85-millions-de-dollars_sto5177903/story.shtml, consulté le 15/04/16.

ce travail, nous veillerons à étudier les modèles d'affaires de ces applications mobiles qui reposent essentiellement sur les données personnelles de leurs utilisateurs.

Chapitre 1. Les données personnelles et la vie privée, un travail de définitions nécessaire

L'utilisation des données personnelles par les entreprises ne date pas de l'ère numérique mais remonte aux prémisses du marketing moderne. Néanmoins, le web et les smartphones ont ouvert la voie à de nouvelles pratiques concernant tant la captation que le traitement des données recueillies sur les consommateurs grâce à de nouveaux outils toujours plus performants. Ces usages ont alors soulevé d'importantes questions du point de vue de la vie privée des individus.

Avant de traiter plus en avant les tenants et les aboutissements de l'utilisation des données personnelles des individus, un travail de définition préliminaire doit être mené. En effet, derrière les notions de « donnée personnelle » et de « vie privée », il est possible de mettre en lumière une pluralité de définitions souvent différentes, ou pis encore, parfois contradictoires. Dans le cadre de ce mémoire, reposant sur l'étude d'un grand nombre d'études anglo-saxonnes, les notions de *personal data* et d'*online privacy* ont été respectivement traduites par « données personnelles » et « vie privée en ligne ».

Section 1 – Une typologie des données

Selon Pierre Delort, une donnée est une information ayant une utilité. Cette transformation nécessite « un coût, a minima, de capture, de transmission et de stockage »[23]. Etymologiquement, le terme « donnée » vient du latin *latum* et signifie « ce qui est donné ». Cette origine de la notion permet de mettre en lumière une autre caractéristique essentielle d'une donnée : elle est construite, soit par l'Homme, soit par la Machine. Au regard de ces premiers éléments de définition, une donnée brute ou naturelle n'existe pas. L'ouvrage

[23] DELORT, Pierre, *Le Big Data*, Presses Universitaires de France, 2015.

collectif *Raw Data is an Oxymoron* édité par Lisa Gitelman vient notamment appuyer ce précédent constat[24].

A l'heure du Big Data, nous l'énoncions précédemment, le nombre de données a connu une augmentation exponentielle ces dernières années. Cette multiplication s'est également accompagnée d'une diversification importante tant en termes de caractéristiques propres que de modes de production. Par souci de temps, nous n'énoncerons ici que la distinction entre les données structurées, les données semi-structurées et les données non-structurées. La distinction mise en avant ici repose sur leur structuration même. Pour l'exemple, une donnée issue d'une base de données est qualifiée de donnée structurée alors qu'une donnée produite depuis les réseaux sociaux (un message Facebook par exemple) ne répond pas à une structure propre.

A) Qu'appelle-t-on une « donnée personnelle » ?

Ce travail vise à étudier une catégorie spécifique de donnée : les données personnelles (ou, en anglais, PII pour « *Personally Identifiable Information* »). Selon la définition de Fabrice Rochelandet, issue de son ouvrage *Economie des données personnelles et de la vie privée*, « Les données personnelles constituent […] des biens informationnels spécifiques combinant une ou plusieurs caractéristiques individuelles de personnes identifiées avec un 'support' prenant la forme d'une série d'octets numérisant ces informations à une date donnée »[25]. D'autre part, l'article 2 de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés énonce : « Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne »[26]. Grâce à ces deux exemples de définitions des données personnelles, il est possible de distinguer un

[24] Ouvrage collectif édité par GITELMAN, Lisa, Raw Data Is an Oxymoron, the MIT Press, 2013.
[25] ROCHELANDET, Fabrice, *Economie des données personnelles et de la vie privée*, éditions La Découverte, 2010.
[26] Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, https://www.cnil.fr/loi-78-17-du-6-janvier-1978-modifiee, consulté le 28/03/16.

élément caractéristique par rapport aux autres types de données : une donnée personnelle concerne directement ou indirectement un individu.

Au sein même de cette catégorie de données personnelles, il est également possible de souligner la construction de différentes typologies. Prenons l'exemple de la typologie définie par l'OCDE dans son rapport « Exploring the Economics of Personal Data : A Survey of Methodologies for Measuring Monetary Value » datant de 2013 :

> *User generated content*, including blogs and commentary, photos and videos, etc. *Activity or behavioural data*, including what people search for and look at on the Internet, what people buy online, how much and how they pay, etc. *Social data*, including contacts and friends on social networking sites; Location data, including residential addresses, GPS and geo-location (e.g. from cellular mobile phones), IP address, etc. *Demographic data*, including age, gender, race, income, sexual preferences, political affiliation, etc. *Identifying data of an official nature*, including name, financial information and account numbers, health information, national health or social security numbers, police records, etc.[27]

Cette typologie vise à faire prendre conscience d'une large diversité des données personnelles. Ne se réduisant pas seulement au nom ou au prénom d'un individu, l'identification d'une personne passe également par des données concernant ses appareils ou ses usages par exemple. En poursuivant l'analyse, il est également possible de distinguer les données personnelles identifiantes des données comportementales. Selon le rapport du CIGREF intitulé « L'économie des données personnelles : les enjeux d'un business éthique », les premières qualifient les données rattachées directement à l'identité d'une personne (nom, adresse, e-mail, situation familiale…) alors que les secondes sont rattachées à l'ensemble des comportements d'un individu[28].

[27] « Exploring the Economics of Personal Data : A Survey of Methodologies for Measuring Monetary Value », OECD Digital Economy Papers, No. 220, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/5k486qtxldmg-eng

[28] Rapport du CIGREF, « L'économie des données personnelles : les enjeux d'un business éthique », www.cigref.fr/wp/wp-content/uploads/2015/11/CIGREF-Economie-donnees-perso-Enjeux-business-ethique-2015.pdf, consulté le 25/01/16.

B) Une pluralité de modes de production des données personnelles

Suite aux éléments de définition précédents, il est nécessaire de mettre en avant les moyens de production des données personnelles. En effet, ces dernières peuvent être produites tant par les individus que par les machines. Dans un premier temps, leur production par les individus peut se faire de façon non intentionnellement. C'est ce qu'on a appelé la production de « traces numériques » (ou « *digital footprints* » en anglais) par les individus. Ces traces numériques, définies par Alain Mille comme « constituées d'empreintes numériques laissées volontairement (ou non ?) dans l'environnement informatique à l'occasion de processus informatiques »[29]. Au sein du même texte, Alain Mille évoque le discours de Bernard Stiegler prononcé lors de la conférence www2012 à propos des traces numériques :

> Toute activité médiée par l'environnement informatique produit des traces numériques. Il s'agit du dernier stade du processus de grammatisation entamé avec l'écriture et décrit par Sylvain Auroux. *Ces traces-écritures sont produites de manière indirecte par l'usage de l'environnement informatique.* Ce sont les marques (événements, écrits, dépôts, etc.) produites par les interactions entre l'utilisateur et l'environnement qui forment les traces, exploitées de plus en plus par les algorithmes pour intervenir sur la manière dont les interactions dans l'environnement seront possibles (recommandation, adaptation, personnalisation, contrôle, etc.).[30]

Les individus peuvent également produire des données de façon intentionnelle. Remplissage d'un formulaire, ajout de photos, rédaction d'un message… toute action des individus visant à alimenter une base de données peut ainsi être considérée comme une production volontaire de données personnelles. Par souci de temps, ce travail ne s'attachera pas à traiter cette question spécifique. A l'inverse, avec l'exemple des applications mobiles de running, ce mémoire vise à traiter les données personnelles recueillies par les fournisseurs de service à partir des informations transmises suite aux activités des individus. Cette captation n'est pas le produit d'une action intentionnelle des individus. Elle soulève notamment la question de la place de la vie privée des individus et de leur capacité, ou de leur incapacité, à conserver une certaine intimité dans leurs actions.

[29] MILLE, Alain, « Des traces à l'ère du Web », Intellectica, 2013/1, 59, pp 7-28.
[30] *Ibid*.

Section 2 – De la vie privée à la vie privée en ligne

Nous l'énoncions en introduction, de nombreux faits d'actualité récents ont réintroduit la question de la vie privée au sein des débats publics. Avec l'affaire Snowden en tête, les individus ont pu être soumis à des flux d'informations croissants portant spécifiquement sur ces questions mais plus précisément sur celle de leur vie privée en ligne. Avec les réseaux sociaux tels que Facebook ou Twitter par exemple, la notion d'*online privacy* a été abondamment traitée par un grand nombre de chercheurs. Ainsi, du concept de vie privée en général à celui de vie privée en ligne en particulier, plusieurs considérations préliminaires doivent être posées. L'une des raisons à cela est la nature fondamentalement polysémique du terme « *privacy* » et des différences existantes entre le terme anglais et son équivalent en français.

A) La vie privée, une pluralité de définitions pour une même notion

Du latin *privatus* signifiant « séparé de, dépourvu de », la notion de vie privée est intimement liée à celle de données personnelles et de leur traitement par des acteurs tiers. Selon Daniel J. Solove, le concept de vie privée est « trop compliqué pour être réduit en une seule essence »[31]. Néanmoins, selon une récente parution dans la revue University of Pennsylvania Journal of international Law, il est possible de définir une typologie précise de la vie privée. Reposant sur des travaux de recherche, cette typologie est composée de plusieurs types de vie privée : « *bodily privacy* », « *spatial privacy* », « *communicational privacy* », « *proprietary privacy* », « *intellectual privacy* », « *decisional privacy* », « *associational privacy* » et « *behavorial privacy* »[32]. Alessandro Acquisti, dans son article intitulé « The economics of Privacy », résume ainsi les précédents travaux de définition :

> It has been described as the protection of someone's personal space and their right to be left alone (Warren and Brandeis, 1890); as the control over and safeguard of personal information (Westin, 1967); or as an aspect of dignity, autonomy and ultimately human

[31] SOLOVE, Daniel J., "A Taxonomy of Privacy", University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, Janvier 2006.
[32] KOOPS, Bert-Jaap, NEWELL Bryce Clayton, TIMAN, Tjerk, SKORVANEK, Ivan, CHOKREVSKI, Tom et GALIC, Masa, "A Typology of Privacy", University of Pennsylvania Journal of International law, 24 mars 2016.

> freedom (Schoeman, 1992). With seemingly different, *all of these definitions relate to the boundaries between the self and the others, between private and public*. As the individuals and as consumers, we constantly navigate those boundaries, and the decisions we make about them determine tangible and intangible benefits and costs, for ourselves and for society.[33]

Ces dernières années, le champ d'étude de la vie privée a été très actif. L'un des fameux auteurs ayant traité cette question est Richard Posner, actuel juge à la Cour d'appel des Etats-Unis pour le septième circuit. Dans son article « The Right of privacy », il y définit la vie privée comme le fait de retenir ou, à l'inverse, de divulguer des informations (« *witholding or concealment of information* »)[34].

B) Vers une remise en cause de la vie privée en ligne ?

Avec l'essor de l'ère numérique et de la constitution d'un espace dit « virtuel », la notion de vie privée a acquis une nouvelle dimension. De la même manière que la notion de vie privée, il est possible de définir la vie privée en ligne comme la capacité de retenir ou de divulguer ses informations de façon maîtrisée. Selon Gergely Biczok et Pern Hui Chia, la vie privée en ligne doit être abordée suivant trois dimensions essentielles : « *Personal: Potential loss of information about a user and his behavioral data: Relational: Revelation of how a user relate to and communicate with others. Spatial: Invasion of the virtual space of an online user* »[35]. Au vu des éléments précédents, la protection de la vie privée dans la vie de tous les jours et en ligne a été perçue comme fondamentale, comme l'illustre la résolution 68/167 des Nations Unies datant de décembre 2013. Cette résolution stipule que les droits des individus hors ligne doivent également être assurés en ligne et que les Etats doivent respecter et protéger le droit à la vie privée en ligne[36].

Dans ce contexte de développement d'internet et des usages de plus en plus intensif des données personnelles, une crise de la vie privée a pu être soulignée. Certains auteurs ont parlé d'une « mort de la vie privée en ligne ». Ils pointent notamment du doigt la collecte et

[33] ACQUISTI, Alessandro TAYLORE, Curtis et WAGMAN, Liad, http://people.duke.edu/~crtaylor/Privacy_Survey.pdf
[34] POSNER, Richard A., "The Right of Privacy", University of Chicago Law School, 1977.
[35] BICZOK, Gergely et HUI CHIA, Pern, "Interdependent Privacy: Let Me Share Your Data, Financial Cryptography and Data Security, Volume 7859 of the series Lecture Notes in Computer Science, pp 338-353.
[36] "The Right to Privacy in the Digital Age", Nations Unis, http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx, consulté le 29/04/16.

l'utilisation des données personnelles par les firmes et gouvernements. Selon Martin Enserink et Gilbert Chin, « *Privacy as we have know it is ending, and we're only beginning to fathom the consequences* »[37]. Après ces considérations générales sur ces deux notions de données personnelles et de vie privée en ligne, il nous faut désormais étudier leurs applications au champ d'étude de ce mémoire, c'est-à-dire les applications mobiles de course à pied disponibles sur smartphones. Existe-t-il des caractéristiques spécifiques ? Les usages sont-ils fondamentalement différents par rapport à ceux observés sur les ordinateurs de bureau ?

Section 3 – Cas particulier des applications mobiles de running

Définis comme des téléphones mobiles associant des fonctions téléphoniques avec d'autres fonctions allant de l'appareil photographique à la navigation web en passant par la messagerie électronique, les smartphones ont connu un essor important en termes d'adoption par les individus et de développement par des entreprises spécialisées. Le premier « smartphone » fut le *Simon*, commercialisé par IBM à partir de 1992. La sortie du premier iPhone en 2007 marqua la popularisation de ce type d'appareil et son adoption par un nombre croissant d'utilisateurs. Plus récemment, le smartphone s'est imposé comme le premier appareil de téléphonie mobile, au détriment de son prédécesseur, le *featured phone*.

Véritable ordinateur de poche, les capacités de calcul d'un smartphone permettent à leurs utilisateurs d'installer des applications, c'est-à-dire des logiciels téléchargés via des App Stores et qui permettent de répondre à un ou plusieurs besoins limités. Il a été possible d'assister à une récente explosion du nombre d'applications mobiles disponibles au téléchargement, gratuites comme payantes. Nous aborderons plus en détail ce point mais il est d'ores et déjà possible d'affirmer que cette gratuité n'est qu'apparente. En effet, même si les utilisateurs ne dépensent pas d'argent lors du téléchargement de ces applications gratuites, ils acceptent néanmoins de transmettre une partie plus ou moins importante de leurs données personnelles aux entreprises en charge du développement de ces applications.

[37] IGO, Sarah E., "The Beginnings of the End of Privacy", The Hedgehog Review: Vol. 17, No. 1, 2015.

A) Une définition possible des applications mobiles de running

Comme énoncé précédemment, ce travail vise à traiter d'un type particulier d'applications mobiles, celui des applications mobiles de course à pied. S'inscrivant dans la catégorie « santé et bien-être », ces applications mobiles offrent à leurs utilisateurs l'enregistrement de leurs performances sportives, le suivi de ces dernières, des programmes d'entrainements, etc. Utilisées au cours de chaque exercice de leurs utilisateurs, ces applications permettent la captation d'un grand nombre de données personnelles. Selon une étude de la Federal Trade Commission menée par Jah-Juin Ho en 2014 ayant examiné douze applications mobiles de santé et de fitness, il a été démontré qu'une multitude de données personnelles ont été transmis à soixante-seize « *third parties* », c'est-à-dire à d'autres entreprises ou organisations[38]. L'année précédente, une autre étude, commandée par le journal The Financial Times auprès du groupe Evidon, a mis en avant le fait suivant : plus d'une vingtaine d'applications transmettaient des données personnelles recueillies auprès de leurs utilisateurs à plus de soixante-dix entreprises[39].

Suivant ce constat, il serait intéressant de connaître la nature des données personnelles collectées. Comme nous l'énoncions précédemment, les smartphones sont dotés d'un grand nombre de capteurs, allant d'un microphone à un GPS en passant par une caméra. Les applications mobiles ont ainsi poussé de plus en plus loin l'ensemble des capacités individuelles de ces différents capteurs mais aussi ont innové en croisant les informations collectées. Le résultat a été la collecte de nouveaux types de données personnelles.

Depuis 2011, la CNIL, en partenariat avec Inria, a mis en place un projet de recherche portant sur les données personnelles collectées par les applications mobiles. Appelé Mobilitics, ce projet vise à « mieux connaître les smartphones, ces objets utilisés quotidiennement par des dizaines de millions de français et qui restent de véritables boîtes noires pour les utilisateurs, les chercheurs et les autorités de régulation »[40]. Suite à la publication des résultats généraux, incluant ceux de l'étude des applications iOS réalisée entre novembre 2012 et janvier 2013 et ceux de l'étude des applications Android analysées de juin à septembre 2014, il a pu être constaté qu'une partie des applications étudiées accédaient à un

[38] MOTTL, Judy, "FTC: Health, fitness apps share user info with vendors", Fierce Mobile Healthcare, http://www.fiercemobilehealthcare.com/story/ftc-vendors-sharing-mhealth-fitness-app-data/2014-05-12, consulté le 27/04/16.
[39] STEEL, Emily et DEMBOSKY, April, "Health apps run into privacy rugs", The Financial Times, Septembre 2013.
[40] Voir Annexe 5

grand nombre de données personnelles : numéro d'identification de l'appareil (UDID ou Android ID), géolocalisation, carnet d'adresses, calendrier, nom de l'appareil, nom de l'opérateur, etc[41].

B) La question des données sensibles

Suite à cette première typologie, Il est essentiel d'aborder la question d'une catégorie spécifique de données personnelles : celle des données sensibles. Dans son article 8, la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés stipule qu'il « est interdit de collecter ou de traiter des données à caractère personnel qui font apparaitre, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci ». La question qui se pose donc est la suivante : les applications mobiles de running collectent-elles des données sensibles, et plus particulièrement des données relatives à la santé de ses utilisateurs ? Selon l'article 8 de la directive 95/46/EC 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 stipule quant à elle que les données médicales sont une catégorie spéciale de données dont une protection plus élevée s'applique en raison de leur nature. Selon le groupe de travail « Article 29 » sur la donnée personnelle, institué par cette même directive, il existe trois scénarios possibles où les données personnelles sont des données médicales : « *1. The data are inherently/clearly medical data. 2. The data are raw sensor data that can be used in itself or in combinaisons with other data to draw a conclusion about the casual health status or health risk of a person. 3. Conclusions are drawn about a person's health status or health risk (irrespective or whether these conclusions are accurate or inaccurate, or illegitimate, or otherwise adequate or inadequate* »[42].

[41] La lettre innovation et prospective de la CNIL, « Mobilitics, saison 2 : Les smartphones et leurs apps sous le microscope de la CNIL et d'Inria, n°08, novembre 2014, https://www.cnil.fr/sites/default/files/typo/document/Lettre_IP_N-8-Mobilitics.pdf, consulté le 09/03/16.

[42] Annexe de la directive 95/46/EC, « health data in apps and devices", http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf, consulté le 17/04/16.

Pour Alvaro Bedoya, directeur exécutif du Center of Privacy and Technology de l'Université américaine Georgetown : « *I think the key risk that we have is that we will create a pool of extremely sensitive health data that is totally unregulated and that is shared broadly without our knowledge and used in ways that we do not know* ». Dans un entretien accordé au site CIO.com, il poursuit :

> Pooled together, those data points could provide potential indicators for conditions such as obesity and Alzheimer's. But the market for that data is fairly opaque […] that *health information in the hands of data brokers could be sold to businesses for dubious purposes*, such as insurances companies that might deny applicants coverage or charge steeper premiums based on information collected through health apps.[43]

Au vu des éléments précédents, il est donc possible d'affirmer que les applications mobiles de running ont accès à des données personnelles initialement non sensibles. Néanmoins, après un traitement et une analyse croisée de ces données personnelles, il est finalement possible de les définir comme des données sensibles.

Ce travail de définitions nous a conduit à mettre en lumière les premiers enjeux de la collecte et du traitement des données à caractère personnelles vis-à-vis de la vie privée des individus. En apparence gratuites, et c'est notre point suivant, les applications mobiles de running ont développé des modèles d'affaires reposant sur les données personnelles de leurs utilisateurs. Outre la question des pratiques de monétisation des données personnelles, il sera également crucial d'aborder la question de leur valeur.

Chapitre II. De l'apparente gratuité des services à des modèles d'affaires reposant sur les données personnelles

L'explosion du nombre d'applications mobiles de running illustre bien les pratiques actuelles concernant les données personnelles. La grande majorité de ce type d'applications sont accessibles gratuitement et très facilement par les utilisateurs. Derrière cette apparente gratuité, ce sont les données personnelles recueillies lors de l'inscription et de l'utilisation des services qui permettent de financer les activités des fournisseurs de services.

[43] CORBIN, Kenneth, "What happens with data from mobile health apps?", CIO.com, www.cio.com/article/2903573/healthcare/what-happens-with-data-from-mobile-health-apps.html, consulté le 17/04/16.

Pour L. Gordon Crovitz, « *People also seem to understand there's no such thing as a free lunch, even online, summarized by the truism 'If you're not paying for something, then you're not the customer – you're the product being sold* »[44]. Cette citation met en lumière un modèle économique dit « *biface* » semblable à ceux adoptés par les plateformes telles que Facebook et Google par exemple. En effet, les consommateurs du service ne sont pas les clients finaux mais bien des fournisseurs de données[45]. Les clients finaux sont véritablement les « *data brokers* » ou courtiers des données, c'est-à-dire les entreprises qui se sont spécialisées dans l'achat et la revente des données[46]. Dans un article intitulé « Privacy Is the New Money, Thanks to Big Data », un contributeur du blog « Opinion » du magazine Forbes parle de « Grand Marché » (En anglais, «*The Grand Bargain* ») pour désigner cette tendance : les données personnelles sont devenues une nouvelle monnaie pour les individus afin d'accéder à de nouveaux services, auparavant payants. Il cite notamment l'exemple des GPS. En effet, ces dernières années, il a été possible d'accéder à des services GPS gratuitement : Google, Waze…[47]. Après ce constat initial, Il est nécessaire de mettre en lumière l'usage commercial des données personnelles recueillies pour ensuite aborder les questions centrales de valeur de ces données et de leurs éventuelles externalités.

Section 1 – Le prix de la gratuité : état des lieux des usages des données personnelles

Dans leur article de recherche « How Small is Zero Price? The true value of free products », deux chercheurs du MIT (Kristina Shampan'er et Dan Ariely) ont tenté de démontrer les éléments suivants : confrontés au choix entre un produit gratuit et un produit payant, les individus réagiraient au produit gratuit comme si son prix « zéro » signifiait un coût d'achat réduit mais aussi une valeur accrue par rapport au produit payant[48]. Dans le

[44] L. Gordon Crovitz, « Will Regulators Unfriend Facebook?, Wall Street Journal, 21 mai 2012.
[45] CHIGNARD, Simon et BENYAYER, Louis-David, *Datanomics, les nouveaux business models des données*, Editions FYP, 2015.
[46] A Review of the Data Broker Industry : Collection, Use and Sale of Consumer Data for Marketing Purposes, Committee on commerce, science and transporation, US Senate, 2013.
[47] BEN-SHAHAR, Omri, "Privacy Is the New Money, Thanks to Big Data", Contributeur sur le blog Forbes, http://www.forbes.com/sites/omribenshahar/2016/04/01/privacy-is-the-new-money-thanks-to-big-data/#7fce6aaf20c3, consulté le 31/03/16.
[48] SHAMPAN'ER, Kristina et ARIELY, Dan, « How Small is Zero price? The True Value of Free Products", Working Papers, Federal Reserve Bank of Boston, No. 06-16.

même ordre d'idée, David Adam Friedman énonçait le constat suivant : « *Free offers exist to lure potential customers to a specific offering, to bring them to the commercial enterprise where an offering can be presented, or to create an often-hidden psychological tie between customers and the enterprise that helps induce a sale* »[49]. A partir de ces premiers éléments de réflexion, il est possible de faire le lien avec les pratiques actuelles, et plus précisément avec les usages des données personnelles par les applications mobiles offrant des services "gratuits". Quels sont-ils ? Comment définir la valeur des données personnelles ?

A) Un essor des modèles d'affaires reposant sur les données personnelles des utilisateurs

Dans son fameux ouvrage *Free ! Entrez dans l'économie du gratuit* paru en 2009, l'ancien rédacteur en chef du magazine Wired Chris Anderson énonce que :

> « Le gratuit repose sur l'économie des bits et non des atomes. Particularités de l'ère numérique, dès lors qu'une chose devient du logiciel, elle devient inévitablement gratuite – dans son coût, en tout cas, et souvent dans son prix. (Imaginez que le prix de l'acier soit tombé si près de zéro que King Gillette ait pu donner aussi bien le rasoir que les lames et gagner de l'argent sur quelque chose d'entièrement différent – la mousse à raser ?) Ainsi est en train de naître *une économie pesant des milliards de dollars – la première de l'histoire – où le prix de référence est zéro* »[50].

Selon C. Anderson, le modèle de la gratuité est intimement lié à l'ère du numérique et prédisait son essor dans les années à venir. Dans ce même ouvrage, il y développe les quatre configurations de ce modèle : les « subventions croisées directes », le « marché tripartite », le « freemium » et le « don ». L'objet de ce mémoire se focalise principalement sur la deuxième configuration. Avec l'exemple de Google et du marché publicitaire, Chris Anderson met en lumière les interactions entre trois types d'acteurs : les individus-consommateurs, les entreprises souhaitant vendre leurs produits et les entreprises souhaitent promouvoir leurs produits grâce à des publicités ciblées. Ce concept de « marché tripartite » a pu être repris par de nombreuses entreprises au sein de secteurs d'activités pluriels.

[49] FRIEDMAN, David Adam, "Free Offers: A New Look", New Mexico Law Review, Vol. 38, 2008.
[50] ANDERSON, Chris, *Free! Entrez dans l'économie du gratuit*, Editions Broché, 2009.

A partir de ces modèles d'affaires spécifiques à la sphère numérique, il est possible de mettre en lumière des ressemblances avec les pratiques analysées dans ce mémoire. Le secteur de la publicité a connu des évolutions majeures abordées précédemment, a fortiori celle du Big Data. Désormais, les entreprises ont la capacité de capter, de traiter puis de vendre les données personnelles de leurs utilisateurs afin de financer leurs activités. Dans son article « L'économie numérique : la réalité derrière le miracle des NTIC », le professeur et fondateur du Département des communications à l'Université du Québec à Montréal Jean-Paul Lafrance affirme que « toute opération sur Internet laisse des traces et constitue un *trésor de guerre* d'entreprises comme Google, Facebook, Blizzard Entertainment ou Rovio Entertainment à qui appartient Angry Birds »[51].

Ainsi, de la même manière que les faits précédents, les fournisseurs de services sur smartphones ont repris ces modes de fonctionnement afin de financer leurs activités, notamment ceux des applications mobiles de running. Deux études centrales ont été produites ces dernières années sur ces questions. Tout d'abord, TheDataMap est un projet de recherche mené par le Data Privacy Lab, un programme de l'Institute for Quantitative Social Science (IQSS) de l'Université d'Harvard. Il met en lumière la captation des données personnelles des utilisateurs par une multitude d'applications mobiles[52]. On constate par exemple que l'application mobile Nike Running sur Android a envoyé des données sensibles, des données PII (personally identifiable information) et des données comportementales au cours de la période étudiée. De la même manière, l'application Runkeeper a envoyé quatre types de données personnelles tant vers les serveurs primaires que vers des serveurs tiers. Ensuite, l'étude « What They Know – Mobile » a été menée par le Wall Street Journal qui a analysé 101 applications mobiles Android & iOS. Le constat est similaire : une majorité d'applications ont collecté et partagé des données personnelles de leurs utilisateurs. Comme illustration, l'application mobile « MyFitnessPal » a transmis les noms d'utilisateurs, les mots de passe, l'âge et le genre à l'entreprise propriétaire de l'application ou encore le numéro d'identification et la localisation à des entreprises tierces.

L'application mobile de running Runkeeper a récemment fait l'objet de critiques suite à la mise en lumière de pratiques douteuses vis-à-vis de la captation des données personnelles.

[51] LAFRANCE, Jean-Paul, « L'économie numérique : la réalité derrière le miracle des NTIC, Revue française de l'informatione et de la communication, 2013.
[52] Voir Annexe 6

En effet, le Norwegian Consumer Council (ou *Forbrukeradet*) a émis une plainte contre Runkeeper suite à une étude menée avec le SINTEF, une organisation indépendante de recherche scientifique implantée en Scandinavie[53]. Datant du 10 mai 2016, le Norwegian Consumer Council a pointé du doigt deux pratiques. D'une part, Runkeeper était accusé de récupérer les données personnelles de ses utilisateurs, même lorsque ces derniers ne sont pas en train d'utiliser activement l'application. D'autre part, l'application ne supprimait pas les données personnelles que ce soit régulièrement ou à la demande explicite des utilisateurs. Selon le document officiel diffusé par le Norwegian Consumer Council, les données collectées ont ensuite été transmises à des « third party », c'est-à-dire à d'autres entreprises. Pour le directeur technique de l'organisation Finn Myrstad, « *everyone understands that Runkeeper tracks users while they exercise, but to continue to do so after the training session has ended is not okay* »[54]. Présentée à la Norwegian Data Protection Authority, équivalent de la CNIL française, la plainte a notamment permis de mettre en lumière une captation et une utilisation des données personnelles qui pouvaient parfois dépasser le cadre juridique des Etats mais aussi des déclarations faites au sein des différentes « privacy policies »[55]. Nous reviendrons sur ce dernier aspect dans la deuxième partie de ce travail.

B) Quels usages des données personnelles ?

A ce niveau de la réflexion, il est essentiel d'aborder la question de l'usage des données collectées. Selon le cabinet de conseil en stratégie et de conseil en management Bain & Company, l'écosystème des données personnelles peut être schématisé en plusieurs étapes : « *Personal data creation* », « *Storage, aggregation* », « *Analysis, productisation* » et enfin « *Consumption* »[56]. Avec ce schéma en tête, il est donc fondamental de distinguer l'usage des données personnelles par les « data brokers » avec l'usage des données personnelles par les entreprises. Dans le cadre de notre propos, nous n'évoquerons uniquement ce dernier cas en éludant volontairement les pratiques des premiers.

---

[53] PULTIER, Antoine, HARRAND, Nicolas et BAE BRANDTZAEG, Petter, "Report: Privacy in Mobile Apps", http://fbrno.climg.no/wp-content/uploads/2016/03/Report-No_final_rettelse_komprimert.pdf, 01/06/2016

[54] MEYER, David, "This Fitness App Tracks You Too Much, Consumer Advocates Claim", http://fortune.com/2016/05/13/runkeeper-privacy-complaint/, consulté le 16/05/2016

[55] MYRSTAD, Finn Lutzow-Holm,"Complaint concerning the mobile phone app Runkeeper", http://fbrno.climg.no/wp-content/uploads/2016/05/2016-05-10-Complaint-runkeeper-ENG.pdf

[56] Voir Annexe 6

Pour Fabrice Rochelandet, Grazia Cecere et Fabrice Le Guel, « les entreprises collectent des données personnelles sur leurs clients pour les exploiter selon des modalités très différentes : identifier ces derniers, communiquer ou interagir avec eux de façon plus ou moins ciblée, différencier leurs prix ou la qualité de leurs offres en fonction des profils des consommateurs identifiés (marché du crédit bancaire par exemple), animer une communauté en ligne, faciliter l'appariement entre les utilisateurs de leurs services (services de réseautage social ou de rencontre en ligne par exemple), revendre ces données à d'autres firmes »[57]. Cette citation met ainsi en lumière plusieurs domaines d'usages des données personnelles.

Tout d'abord, les données personnelles des individus peuvent être utilisées par les entreprises pour affiner la connaissance de leurs clients dans le but d'offrir un service au plus proche de leurs attentes. Pour Michael McFarland, « *Marketers have an immense appetite for personal information too. They use collective data, along with sophisticated statistical techniques and psychological models, to predict peoples' purchasing preferences and behavior and to identify those factors that most strongly influences consumers' loyalty and choices. They then combine this intelligence with detailed information on specific individuals and subgroups of consumers to try to engage and influence their buying decision* »[58]. Les deux axes essentiels à retenir sont donc, d'une part, une volonté d'anticiper les préférences de consommation des individus et, d'autre part, de définir les facteurs de choix de ces mêmes individus. Ces dernières années, la captation et le traitement des données personnelles par les entreprises a permis le développement d'un marketing dit « *one-to-one* ». Il s'agit d'offrir aux consommateurs des produits et des services extrêmement personnalisés. Outre le ciblage de l'offre, ces pratiques permettent également de définir la bonne temporalité. Comme l'énonce Michael McFarland, l'objectif commun est bien d'influencer la prise de décision des individus dans leurs achats. D'une façon similaire, la mission d'expertise sur la fiscalité du numérique de 2013 affirmait que :

> Les données, notamment les données personnelles, sont la ressource essentielle de l'économie numérique. Elles permettent aux entreprises qui les collectent de *mesurer et d'améliorer les performances d'une application, de personnaliser le service rendu, de recommander des achats à leurs clients, de soutenir des efforts*

[57] GRAZIA, Cecere, LE GUEL, Fabrice et ROCHELANDET, Fabrice, « Les modèles d'affaires numériques sont-ils trop indiscrets ? Une analyse empirique », Réseaux 1/2015 (n°186), p.77-101.
[58] MCFARLAND, Michael, « Unauthorized Transmission and use of Personal Data", https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/unauthorized-transmission-and-use-of-personal-data/, consulté le 05/05/16.

> *d'innovation donnant naissance à d'autres applications, de prendre des décisions stratégiques.* Les données peuvent également être valorisées auprès de tiers concessionnaires de leur utilisation, notamment à travers les modèles de plateforme logicielle. D'une manière générale, les données sont le levier qui permet aux grandes entreprises du numérique d'atteindre de grandes échelles et des niveaux élevés de profitabilité.[59]

D'un point de vue économique donc, les données personnelles représentent un véritable « levier » pour les entreprises. L'objectif est de financer les activités des organisations et d'assurer leur croissance, interne comme externe. Nous énoncions en introduction le rachat d'applications mobiles de running par des équipementiers sportifs. Au vu des éléments énoncés précédemment, il est désormais possible de mieux cerner les enjeux fondamentaux que représentent les données personnelles pour ces derniers. Ces applications mobiles permettent l'accès à des données extrêmement précises sur les pratiques sportives de leurs utilisateurs : régularité, intensité, etc. Il est alors possible d'adapter l'offre par rapport à ces valeurs afin tant de conquérir une part plus importante de consommateurs que de tendre vers une personnalisation très précise.

D'autre part, les données personnelles ont également permis l'essor de pratiques appelées « *Advertising targeting* », autrement dit la diffusion de publicités ciblées. Définie comme « *The concept of targeted advertising basically includes the compilation of detailed information about consumers and their preferences in using the Internet or consuming other media for the purpose of providing them with individualized advertisements* » par Christian Schlee, la publicité ciblée a connu un âge d'or avec l'essor des services Google AdSense et Adwords. Toujours selon C. Schlee, "*the key asset for targeted advertising is the hability to identify single users and collect data about their consumption behavior*"[60]. Avec les publicités ciblées, les données personnelles visent à identifier les individus avec une grande précision. L'objectif est, ici encore, de tendre vers des services personnalisés en fonction des individus-cibles. A l'heure actuelle, il existe trois catégories de ciblage publicitaire : le « *Behavorial targetting* », qui est basé sur l'historique web de l'utilisateur, le « *Contextual targeting* », basé

[59] COLLIN, Pierre et COLIN, Nicolas, Mission d'expertise sur la fiscalité du numérique de 2013, http://www.economie.gouv.fr/files/rapport-fiscalite-du-numerique_2013.pdf

[60] SCHLEE, Christian, *Targeted Advertising Technologies in the ICT Space : a Use Case Driven Analysis*, Springer Science & Business Media, 2013.

sur le contenu affiché par l'utilisateur et le « *Demographic targetting* », qui est basé sur l'âge, le genre, les revenus, la mobilité… de l'utilisateur[61].

La collecte et le traitement des données personnelles ont donc ouvert la voie à de nouveaux modèles d'affaires pour les entreprises. Ces dernières années, un large nombre d'acteurs du numérique sont passés à ces types de modèles d'affaires, de Facebook à Uber en passant par Amazon et Airbnb. Dans le secteur du mobile, les développeurs d'applications ont également repris les modèles économiques qui existaient sur le web. Contrairement aux données recueillies en ligne, les données personnelles des « mobinautes » ont pu être qualifiées de plus denses, notamment grâce aux capteurs intégrés aux smartphones. De la géolocalisation au numéro de téléphone en passant par le numéro d'identification des téléphones, les fournisseurs de services de type applications mobiles ont désormais accès à une source de données à forte valeur ajoutée. Cette valeur des données personnelles est-elle véritablement quantifiable ? Si oui, quelles nomenclatures ont pu être utilisées afin de définir avec précision la valeur d'un ensemble défini de données personnelles ?

Section 2 – Valeur et externalités des données personnelles

Au cours du mois de mars 2014, l'étudiant Shawn Buckles a mis en vente l'ensemble de ses données personnelles en ligne: ses emails, ses préférences de consommateur, son historique de navigation… Pour la somme de 350€, c'est la structure TheNextWeb qui a finalement remporté les enchères. Selon les dirigeants de ce site web d'information américain, les données personnelles seront utilisées dans le but d'illustrer les enjeux de la vie privée en ligne. Derrière cette démarche, Shawn Buckles a souhaité mettre en avant la monétisation des données personnelles et leur potentielle valeur monétaire. En effet, selon Mireille Hildebrandt, Kieron O'hara et Michael Waidner, « *the value of personal data can be understood in two ways: as an invaluable asset that is intrinsically linked to the individual person, and as a quantifiable variable that can be traded against various types of services and even money* »[62]. Dans le cadre de ce mémoire, nous nous attacherons à la seconde

[61] TSELIOS, S., PERKUHN, H., VANDIKAS, K. et KAMPMANN, M., « Targeted Mobile Advertisement in the IP Multimedia Subsystem", in XIAN-SHENG, Hua, *Online Multimedia Advertising : Techniques and Technologies*, IGI Global, 2010.

[62] HILDEBRANDT, Mireille, O'HARA, Kieron et WAIDNER, Michael, "Introduction to The Value of Personal data", Digital Enlightenment Forum Yearbook 2013, 2013.

définition proposée ci-dessus. En effet, avec l'émergence du « Big Data » et le passage d'une économie de rareté à une économie de l'abondance, les fondements « classiques » de la valeur en économie - c'est-à-dire le travail, la rareté et l'utilité - ont pu être remis en cause avec les données personnelles. Considérées par le World Economic Forum comme une « nouvelle catégorie d'actif » (ou « *new asset class* » en anglais), les données personnelles représentent une valeur fondamentale non seulement pour les entreprises mais aussi pour les institutions publiques par exemple.

A) Une difficile mesure de la valeur des données

Néanmoins, et notamment selon le rapport « Beyond Goods and Services: The (Unmeasured) Rise of the Data-Driven Economy » écrit par Michael Mandel, la mesure de la valeur des données personnelles est une question complexe car elles ne s'insèrent pas dans la traditionnelle dichotomie des biens et des services :

> « *Data is neither a good or service. Data is intangible, like a service, but can easily be stored and delivered far from its original production point, like a good.* What's more, the statistical techniques that have been traditionally used to track goods and services don't work well for data-driven economic activities. The implication is that the key statistics watched by policymakers – economic growth, consumption, investment, and trade – dramatically understate the importance of data for the economy"[63].

Les données personnelles ne peuvent donc pas être affiliées, dans un premier temps, à des biens. Non épuisable, les données personnelles ne se détruisent pas lors de leur « consommation » par les entreprises tierces. Dans un second temps, la valeur d'une donnée n'est pas définie en fonction de sa nature mais bien en fonction de sa circulation. Selon Simon Chignard et Louis-David Benyayer, la « valeur des données est plutôt une valeur d'immédiateté »[64]. En effet, il est possible de noter qu'une donnée ancienne est beaucoup moins intéressante pour une entreprise par rapport à une donnée personnelle récente.

Ces tentatives de définir une échelle de valeur des données personnelles sont, en définitive, intrinsèquement liées aux externalités qu'elles engendrent, positives comme

[63] MANDEL, Michael, "Beyond Goods and Services: The (Unmeasured) Rise of the Data-Driven Economy", Policy Memo, Progressive Policy Institute, 2012.
[64] CHIGNARD, Simon et BENYAYER, Louis-David, Datanomics, les nouveaux business models des données, Editions FYP, 2015.

négatives. Dans son rapport datant de 2013, l'OCDE affirmait que « *many of the uses of data that create direct value don't necessarily involve a market transaction or can be measured by a market transaction – but the economic and social impact is direct* »[65]. En effet, la création de valeur des données ne fait pas forcément suite à une transaction où un « panier » de données est échangé contre une somme d'argent donnée. Néanmoins, la passation de ce même panier peut avoir des retombées économiques ou sociales importantes.

B) Les externalités des données personnelles

Au sein de la préface de la deuxième édition de l'ouvrage *L'âge de la multitude*, co-écrit par Nicolas Colin, inspecteur des finances et membre de la Commission Nationale de l'information et des libertés (CNIL) et Henri Verdier, directeur de la mission Etalab qui est en charge auprès du Premier ministre français des politiques de la donnée et des politiques d'*open government*, le constat suivant est dressé :

> D'un côté, la collecte des données [personnelles] est un terme essentiel de l'alliance conclue entre la multitude et les entreprises qui collectent des données sur elle : c'est parce qu'elles connaissent mieux les individus que ces entreprises peuvent mieux les servir en baissant leurs prix, en personnalisant leur proposition de valeur ou en soutenant une dynamique constante d'innovation. De l'autre côté, l'ampleur de la collecte des données personnelles est à ce point inédite que beaucoup de questions restent sans réponse. L'impératif de la confiance est-elle un tempérament suffisant aux excès de la collecte des données ? La multitude sait-elle se défendre contre les entreprises tentées par la prédation ? Comment adapter le droit des données personnelles à une économie de plus en plus globale et de moins en moins européenne ? De notre capacité à trancher ces débats dépend notre développement économique futur.[66]

Rédigée trois ans après la première édition, cette préface met en lumière les enjeux de la collecte des données personnelles par les entreprises et leur utilisation à des fins commerciaux. Ces pratiques ont pu conduire à parler de véritables externalités de la donnée. Selon la définition de l'OCDE, « *externalities refers to situations when the effect of production and consumption of goods and services imposes costs or benefits on others which*

[65] OECD, « Exploring the Economics of Personal Data : A Survey of Methodologies for Measuring Monetary Value », OECD Digital Economy Papers, No. 220, OECD Publishing, Paris, 2013

[66] COLIN, Nicolas et VERDIER, Henri, L'âge de la multitude. Entreprendre et gouverner après la révolution numérique, Editions Armand Colin, 2012.

are not reflected in the prices charged for the goods and services being provided »[67]. Il est ainsi possible d'appliquer cette notion d'externalité à celle de la vie privée. En effet, selon M. MacCarthy, la décision de certains individus de divulguer une partie de leurs données personnelles à des acteurs tiers peut conduire à la divulgation de données personnelles d'autres individus n'ayant pas donné leur accord[68]. D'un côté, les externalités négatives ont pu être régulièrement pointées du doigt, notamment concernant une atteinte à la vie privée des individus. Dans l'ouvrage *Digital Identity Management* de Maryline Laurent et de Samia Bouzefrane, les externalités négatives évoquées sont plurielles : « *identity theft, other forms of third party data use for questionable purposes such as spamming or direct marketing ; loss of personal data such as credit card number due to a lack of security of the servers where the data are stored* »[69]. Au cours des entretiens menés dans le cadre de ce mémoire, plusieurs individus interrogés ont volontairement mis en avant leurs craintes des externalités précédentes. L'une d'entre elles a été la réception de nombreux « spams » ou encore la diffusion de leur adresse personnelle à des personnes mal intentionnées. D'un autre côté, les deux auteures ont également mis en lumière des externalités positives. Selon elles, les données personnelles ouvrent la voie à des pratiques à forte valeur ajoutée pour les entreprises : « *better forecasting of market trends and the development of individual preferences ; better targetting of offers, the development of niches products* »[70]. Avec ces éléments, il est donc possible de soulever des externalités positives et négatives de l'utilisation des données personnelles par les entreprises.

Les questions de données personnelles et de vie privée sont intimement liées. Les applications mobiles de running peuvent être téléchargées gratuitement par les utilisateurs et être utilisés lors de leurs entrainements hebdomadaires. Cette apparente gratuité est permise, nous l'avons vu, par la collecte, la valorisation et l'utilisation des données personnelles de ces mêmes utilisateurs. Cette réflexion nous a conduit à étudier les externalités positives et négatives de ces pratiques sur la vie privée des individus. En définitive, il est possible d'analyser cette acceptation de transmettre ses données personnelles dans le but d'accès à des

[67] Glossary of Industrial Organisation Economics and Competition Law, compiled by R.S. Khemani and D. M. Shapiro, commissioned by the Directorate for Financial, Fiscal and Enterprise Affairs, OECD, 1993.
[68] MACCARTHY, Mark, « New Directions in Privacy: Disclosures, Unfariness and Externalities", Privacy Law Scholars Conference, GeorgeTown University, June 2010, http://www18.georgetown.edu/data/people/maccartm/publication-51099.pdf.
[69] LAURENT, Maryline et BOUZEFRINE, Samia, Digital Identity Management, 1st edition, 2015.
[70] *Ibid*.

bénéfices à court terme. La question qui se pose désormais est donc la suivante : les utilisateurs sont-ils informés de la captation de leurs données personnelles ? Plus encore, dans le cas où les individus sont informés de l'usage de leurs données personnelles, peut-on dire que le choix a été fait de façon rationnelle ? Notion renvoyant à l'économie classique, cette question de la rationalité sera bel et bien le fil rouge de notre seconde partie.

Partie II : De l'homo economicus à l'homo numericus : perception et processus décisionnel des utilisateurs des applications mobiles de running vis-à-vis de leur vie privée

Après avoir vu l'usage des données personnelles par les fournisseurs de services mobiles de type applications, il nous faut s'interroger sur le regard des utilisateurs et des raisons qui les poussent à bénéficier de ces services au détriment de leur vie privée. C'est l'un des objets d'études de l'économie comportementale ou « *behaviorial economics* ». Pour Colin F. Camerer et George Loewenstein, « *at the core of behavioral economics is the conviction that increasing the realism of the psychological underpinnings of economic analysis will improve economics on its own terms – generating theoretical insights, making better predictions of field phenomena, and suggesting better policy* »[71]. Comme son nom l'indique, l'économie comportementale traite donc du comportement des individus dans des situations économiques et se pose contre la théorie classique de la rationalité des agents économiques. En cela, différentes études portant sur la vie privée ont été faites dans le cadre de l'économie comportementale. Par souci de clarté, elles ont différencié deux temps dans leurs analyses avec la perception, ou « *privacy attitudes* » d'un côté, et la prise de décision, ou « *privacy behaviors* » de l'autre.

Tout d'abord, la perception de la divulgation de sa vie privée a été une question abondamment traitée ces dernières années. Elle porte sur la vision mais aussi sur le discours des individus concernant des pratiques parfois discutables. Ensuite, les « *privacy behaviors* » portent plutôt sur les actions et réactions des individus vis-à-vis de ces pratiques. Plus qu'une étude parallèle, ces deux concepts ont pu être traités ensemble afin d'en analyser les relations logiques qui existaientt entre eux. L'idée première venant à l'esprit est bien que si un individu perçoit des manquements à sa vie privée, il agirait en conséquence et ferait tout pour réduire la divulgation de ses informations. Au-delà de ce constat, qui semble suivre une logique admise, les pratiques observées montrent que cela n'est pas toujours ce qui se passe en réalité.

[71] CAMERER, Colin F. et LOEWENSTEIN, George "Behavorial Economics: Past, Present, Future" in *Advances in Behavorial Economics*, Princeton University Press, 2004.

Il est donc nécessaire d'étudier séparément ces deux temps afin de pouvoir, par la suite, en arriver à des éclaircissements concernant les utilisateurs des applications mobiles de running.

Chapitre 1. La perception du risque d'atteinte à la vie privée par les utilisateurs

Avant d'aborder la prise de décision des individus concernant la divulgation ou non d'une partie de leur vie privée, il est nécessaire de traiter de la perception des individus vis-à-vis du risque de divulgation. Au cours de l'histoire des civilisations, les luttes pour acquérir puis conserver sa vie privée ont été plurielles tant par leur localisation géographique que par leur temporalité. A l'ère du numérique, ces luttes n'ont pas disparu. Malgré une différence d'environnement, la sphère numérique a soulevé des enjeux importants concernant la vie privée des utilisateurs.

Avec l'essor du mobile et des applications mobiles, ces mêmes enjeux n'ont pas disparu. Au cours de ces dernières années, plusieurs personnalités, d'Edward Snowden à Glenn Greenwald, ont soulevé les dysfonctionnements des Etats et des grandes firmes mettant à mal notre vie privée. C'est dans ce contexte sensible que les individus ont dû se forger une opinion, tant au cours de leurs années d'enseignement que de leurs temps de formation professionnelle et personnelle. Ainsi, chaque individu se forge sa propre perception des éventuelles atteintes de sa vie privée, en fonction notamment de son niveau de connaissance relatif à ces sujets.

Section 1 – Quel niveau de connaissance des individus concernant la transmission des données personnelles ? L'exemple des messages de pré-téléchargement

Avant d'aborder la question de l'inquiétude de la protection de la vie privée des individus, il est nécessaire de soulever la question du niveau d'information des utilisateurs des applications mobiles concernant la captation, de la valorisation et du partage de leurs données personnelles à des entreprises tiers. En effet, selon l'étude « Internet Privacy Sweep » datant de 2013, 57% des 1013 personnes interrogées ne connaissaient pas ou n'étaient pas sûres de la

nature des informations dont l'application avait accès[72]. Dans le cadre des applications mobiles, il est plus difficile aux fournisseurs de services d'informer efficacement les utilisateurs. Néanmoins, il est possible d'analyser deux éléments à valeur informative : les messages de mise en garde précédant le téléchargement des applications et les politiques de confidentialité accessibles ultérieurement.

A) Nature et usages des messages de pré-téléchargement par les utilisateurs

Tout d'abord, lorsqu'un utilisateur souhaite télécharger une application, il doit se rendre sur un App Store et parcourir l'ensemble des applications mobiles disponibles. Après avoir sélectionné une application en particulier, il accède à une page de présentation affichant des images d'aperçu, des avis d'utilisateurs et un bouton de téléchargement. Avant de pouvoir lancer le téléchargement, l'utilisateur voit apparaître un message lui informant des différentes données accessibles par l'application. Comme illustration, prenons l'exemple du téléchargement de l'application Runstatic. Les utilisateurs doivent autoriser l'accès aux données suivantes : « Historique des appels et des applis », « Identité », « Position », « Photos/multimédia/fichiers », « Micro », « Informations de connexion au Bluetooth » et « Autres ». Ce n'est qu'après avoir cliqué sur le bouton « Accepter » que le téléchargement de l'application peut enfin débuter[73].

Selon l'étude intitulée « Privacy as part of App decision-making process », il est avancé que : « *most users do not pay attention to the permissions screens at install time (83%) and that only three percent of their surveyed users has a good understanding of what the permissions were actually asking for access to* »[74]. Au cours d'un des entretiens qualitatifs, Coralie C. énonçait que « Oui, j'ai lu le message qui s'affiche avant d'avoir téléchargé les différentes applications. Dès que je télécharge une application, je l'accepte… Je l'accepte automatiquement »[75]. Pour Olivia B, le constat est similaire : « Je ne lis jamais les

[72] Study Report on the Privacy Policy Transparency ("Internet Privacy Sweep") of Smartphones Applications, Office of the Privacy Commissioner for Personal Data, Hong Kong, 2013, http://www.pcpd.org.hk/english/publications/files/mobile_app_sweep_e.pdf, consulté le 25/05/16.
[73] Voir Annexe 7
[74] KELLEY, Gage Patrick, CRANOR, Lorrie Faith et SADEH, Norman, "Privacy as part of App decision-making process", 2013.
[75] Annexe 9

messages de pré-téléchargement qui apparaissent juste avant le téléchargement des applications. Je ne le fais pas principalement par fainéantise »[76].

B) De nouvelles contraintes imposées aux fournisseurs de services

Comme expliqué précédemment, les smartphones ne disposent pas de grands écrans qui, contrairement à des ordinateurs portables ou des ordinateurs de bureau, permettent aux utilisateurs d'accéder facilement à un grand nombre d'informations. Avec des usages de plus en plus poussées de ce types d'appareils, les développeurs ont dû faire des choix dans le design et l'expérience utilisateur (En anglais, UX pour *User Experience*). Cette simplification des interfaces a notamment conduit à une réduction voire à une suppression des messages d'avertissements concernant la vie privée des utilisateurs. Ces messages de pré-téléchargement représentent l'un des derniers indicateurs de la nature des données récupérées pour les utilisateurs.

Section 2 – Les politiques de confidentialité comme autre source d'informations

D'autre part, la deuxième source d'information pour les utilisateurs réside au sein des politiques de confidentialité des développeurs ou « *Privacy Policies* ». Bien qu'il s'agisse d'applications mobiles, la plupart des développeurs disposent d'une page web permettant, dans un premier temps, de faire la promotion de leurs logiciels et applications. C'est au sein de ces dernières qu'il est possible d'y retrouver les politiques de confidentialité des entreprises. Elles se présentent généralement sous la forme d'un texte qui vise à présenter comment une organisation capte et diffuse les données personnelles transmises par ses clients. Selon une étude de la Privacy Rights Cleaninghouse menée en 2013 et qui a analysé quarante-trois applications mobiles de santé et de fitness gratuites, seulement 43% des studios de développement fournissaient un lien redirigeant vers une politique de confidentialité. Ce rapport met en avant d'autres conclusions : une grande partie de ces applications transmettent des données personnelles non cryptées sans la connaissance de leurs utilisateurs, une grande

[76] Voir Annexe 12

partie de ces applications sont en lien avec des acteurs tiers sans la connaissance de leurs utilisateurs ou encore 72% de ces applications présentaient des risques moyens voire élevés concernant la vie privée de leurs utilisateurs[77]. Plus encore, le President's Council of Advisors on Science and Technology affirmait en 2014 que « *Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent* »[78]. Portant alors sur les politiques de confidentialité des sites web, ce constat s'applique également à une grande majorité des politiques de confidentialité des applications mobiles.

A) Cas d'étude des politiques de confidentialité des applications mobiles de running

En illustration, la politique de confidentialité de l'application Runstatic est accessible relativement facilement à l'aide d'un lien situé en bas de page. Son point 2.1 déclare que : *« Runstatic collects information from users upon registration on its website and in connection with the use of any Runstatic's applications. The personally identifiable information collected by Runstatic falls in the following categories : first and last name; home or other physical address including street name and name of city or town; email address; miscellaneous workout data, such as length and type of workouts, pulse rates, etc.* ». Concernant l'usage de ces données, le point 4.1 affirme les éléments suivants : « *By registering, the user explicitly agrees that Runstatic shall have the right to use all automatically collected personnally identifiable information, in accordance with the privacy settings of such user, for purposes of the Runstatic applications. Runstatic dones not pass on personally information to third parties, except as required by law or with the explicit consent of the user* ». Il est donc possible de constater un effort de transparence de la part des équipes de développement de Runstatic[79].

[77] Privacy Rights Clearinghouse, "Privacy Rights Clearinghouse Relase Study: Mobile Health and Fitness Apps: What Are the Privacy Risks", https://www.privacyrights.org/mobile-medical-apps-privacy-alert, consulté le 13/03/16.
[78] President's Council of Advisors on Science and Technology, « Report to the President: Big Data and Privacy: A Technological Perspective », 2014.
[79] Politique de confidentialité de l'application mobile Runstatic, https://www.runtastic.com/fr/politique-de-confidentialite, consulté 09/03/16.

Coralie, utilisatrice de plusieurs applications mobiles de ce type, affirme qu'elle n'a jamais lu les politiques de confidentialité. Pour elle, « Non, je n'ai pas lu la ou les politiques de confidentialité. Parce que c'est trop long, parce que j'estime que le fonctionnement de l'application Nike Running est le même que pour toutes les applications. Pour moi, les données que je partage sur cette application-là ne sont pas des données que je considère comme confidentielles »[80]. Au cours de ce même entretien, il a pu être constaté une certaine conscience du manque d'informations relatives à l'utilisation de ses données personnelles. Pour elle, cela n'est pas un enjeu en soi, sauf si cette utilisation se transforme en une « intrusion dans [sa] vie personnelle »[81]. Plus encore, elle l'explique par une impuissance d'ordre technique : « Aujourd'hui, l'usage que je fais d'internet, de mon smartphone… je sais que je ne peux pas cacher mes informations. Ou alors, à ce moment-là, je n'ai pas de profil Facebook, de profil Instagram, de profil Pinterest, d'applications de running… Je n'utilise pas les outils modernes qui sont mis à ma disposition. J'ai conscience que, de toute façon, mes informations sont diffusées. Après, je sais qu'il y a des risques. Le jour où j'aurais des enfants, j'éviterai de poster une photo de mon enfant sur internet par souci de confidentialité. Cela ne me gêne pas plus que ça que mes données personnelles soient utilisées par les marques ». Pour Julie C., le constat est très proche :

> Je ne lis pas vraiment non plus les politiques de confidentialité. En tout cas, je ne l'ai pas fait pour Nike+. Je l'ai ai lu une fois sur Snapchat parce que je faisais une étude dessus et, du coup, j'ai regardé. Mais sinon, non. En fait, c'est trop long, trop compliqué, souvent en anglais. Du coup, quand tu lis qu'en français ou que tu ne maitrises pas trop la langue, c'est un peu compliqué de lire quelque chose en anglais d'aussi difficile. Du coup, je fais « Accepter » direct.[82]

Les politiques de confidentialité ont souvent été accusées d'être délibérément illisibles par la plupart de ses lecteurs en raison d'un vocabulaire trop technique, trop juridique… Suite aux critiques massives, les développeurs de services en ligne et d'applications mobiles ont été amenés à produire des textes plus clairs et plus lisibles. Néanmoins, cette simplification a pu être la source d'omissions nombreuses concernant tant la collecte que la valorisation et la revente des données personnelles. Après avoir rapidement étudié ce niveau d'information des utilisateurs, il est nécessaire de nous tourner vers le rapport qu'entretiennent les utilisateurs

[80] Voir annexe 9
[81] Voir annexe 9
[82] Voir annexe 10

avec la divulgation, ou la non-divulgation, de leur vie privée par les développeurs d'applications mobiles.

B) Un rapport complexe des individus concernant la divulgation de leur vie privée en ligne

Ces dernières années, la notion de « *concern of privacy* » a été étudiée à de nombreuses reprises par des auteurs de divers horizons. Pouvant être traduit par « inquiétude pour le respect de la vie privée » ou encore « souci de la protection de la vie privée », elle a notamment été étudiée à travers le prisme de la psychologie. Le point de départ fut celui du modèle des « *Big Five personality traits* » ou « modèle OCEAN » qui permet de définir cinq dimensions d'une personnalité : l'ouverture à de nouvelles expériences, la conscienciosité, l'extraversion, l'agréabilité et le neuroticisme[83]. Pour certains auteurs, ces cinq traits de personnalité peuvent être considérés comme des facteurs influençant l'inquiétude vis-à-vis du respect de leur vie privée. Par exemple, pour Iris A. Junglas, l'agréabilité, la conscienciosité et l'ouverture à de nouvelles expériences vont de pair avec l'intérêt de certains individus pour des services localisés[84]. Selon Melinda L. Korzaan et Katherine T. Boswell, c'est le trait de personnalité d'agréabilité qui est mis en lumière en tant que facteur du souci de la protection de la vie privée des individus[85].

Comme énoncé précédemment, les questions de la vie privée et des inquiétudes relatives à sa protection ont ressurgi à l'ère du web dit 2.0 mais aussi du web mobile. Dans son rapport « *Rethinking Personal Data : Strenghtening Trust* » réalisé en collaboration avec The Boston Consulting Group en 2012, le World Economic Forum évoque une perte de confiance des individus concernant la collecte, l'utilisation et le partage des données personnelles. Plus spécifiquement, il énonce les éléments suivants :

> Surveys show that individuals are losing trust in how data about the mis being collected, used, shared and combined by both organizations and governments. For example,

[83] EGELMAN, Serge et PEER, Eyal, « Predicting Privacy and Security Attitudes", *ACM SIGCAS Computers and Society*, Volume 45, Issue 1, 2015, pp 22-28.
[84] JUNGLAS, Iris A., JOHNSON, Norman A. et SPITZMÜLLER, Christiane, « Personality traits and concern for privacy : an empirical study in the context of location-based services », *European Journal of Information Systems*, 2008.
[85] KORZAAN, Melinda L et BOSWELL, Katherine T., "The Influence of Personality Traits and Information Privacy Concerns on Behavorial Intentions", Journal of Computer Information Systems, 2008.

> according to the European Justice Commissioner Vivane Reding, 72% of European citizens are concerned that their personal data may be misused, and they are particularly worried that companies may be passing on their data to other companies without their permission. However, a *disconnect exists between what people say and what they do: the world of personal data is no exception. While many people say they care about privacy, they also share information quite widely on social networks and elsewhere online*.[86]

Cette déconnexion entre ce que les individus disent et ce qu'ils font est fondamentale. En effet, notamment au cours des entretiens menés dans le cadre de ce mémoire, il a été constaté un décalage plus ou moins important en fonction des individus mais aussi en fonction du contexte entre les discours et les agissements relatifs à la divulgation de leur vie privée. Plusieurs analyses ont pu être menées. D'un côté, les individus sont considérés comme rationnels alors que, de l'autre, ce décalage est considéré comme une marque d'irrationalité.

Chapitre 2. Le processus décisionnel des individus concernant la divulgation de leur vie privée : entre rationalité et irrationalité

L'utilisation des applications mobiles gratuites implique de transmettre aux entreprises de larges quantités de données concernant tant son identité que son activité quotidienne. Comme nous l'avons présenté précédemment, les données transmises représentent une source d'information et de revenus pour des entreprises tierces. Ces dernières années, les analyses de ces pratiques et de la divulgation de la vie privée des individus ont considéré les données personnelles comme des marchandises qui pouvaient être échangées contre d'autres bien et services. Il est possible de souligner la fameuse expression anglo-saxonne « *Personal data is the new oil of the Internet and the new currency of the digital world* »[87].

Le comportement des individus, lorsqu'il s'agit de céder une part plus ou moins importante de leurs données personnelles à des acteurs tiers, a pu être analysé selon deux visions opposées. D'une part, les individus sont considérés comme des êtres rationnels et cèdent donc intentionnellement une partie de leur vie privée afin d'acquérir un bénéfice équivalent à leurs yeux. D'autre part, et de façon opposée, les individus sont perçus comme

[86] World Economic forum, « Rethinking Personal Data : Strenghtening Trust, http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf, consulté le 26/02/16.
[87] KU Meglena Kuneva, commissaire européenne à la consommation, Speech/09/156, mars 2009, www.europa.eu/rapid/press-release_SPEECH-09-156_en.htm, consulté le 26/02/16.

des personnes irrationnelles, dont les décisions sont notamment guidées par des biais psychologiques.

Section 1 – Les individus rationnels et leur processus de décision concernant leur vie privée

La question de la rationalité est centrale en économie et constitue l'un de ses piliers fondateurs. Pour M. Allais, « un homme réputé rationnel lorsque : a) il poursuit des fins cohérentes avec elles-mêmes b) il emploie des moyens appropriés aux fins poursuivies ». L'expression « *Homo economicus* », dont la paternité revient soit à Vilfredo Pareto soit à John Stuart Mill illustre cette rationalité de l'individu dans ses choix[88]. Elle a pu être reprise, notamment par Luc Wathieu et Allan Friedman en 2007. Selon ces deux auteurs, « *there is a homo economicus behind the privacy concern, not simply a primal fear* »[89]. De fait, de la même manière qu'en économie, l'individu a pu être défini comme un être rationnel lorsqu'il s'agissait de la divulgation ou non de sa vie privée. Suivant la théorie du « *Privacy Calculus* » ou de la « *Social Exchange Theory* », ce dernier agirait donc rationnellement.

A) De la théorie du « Privacy Calculus »…

Au sein de ses différentes œuvres, Bernard Stiegler, philosophe français et fondateur du groupe de réflexion philosophique Ars Industrialis, a étudié la technique et plus précisément internet à travers ce qu'il appelle la pharmacologie. En grec, le « pharmakon » désigne à la fois un remède et un poison. En effet, à ses yeux, internet n'est pas neutre, il est pharmacologique. D'une part, internet est un poison par sa nature de média ouvert et en réseau. Il a permis l'émergence de discours extrémistes et le développement de trafics illégaux divers. Dans le même temps, internet est également décentralisé et a été l'élément qui a favorisé l'expression des minorités. Au cours du colloque Gilbert Simondon tenu en 2013, il évoque les éléments suivants :

[88] STUART MILL, John, *Principles of Political Economy*, 1848.
[89] WATHIEU, Luc et FRIEDMAN, Allan, « An Empirical Approach to Understanding Privacy Valuation", Working Knowledge, Harvard Business School, 2007.

> L'Internet est un « φάρμακον » [pharmakon, ndlr], au sens où Platon le disait de l'écriture, et nous découvrons actuellement cette double face. Le système actuel du Web est dangereux pour le secret, pour l'individuation psychique, pour l'individuation collective, et il en va ainsi parce que l'on ne peut pas et l'on ne doit pas tout soumettre à la calculabilité. Une telle soumission ne peut qu'engendrer une « servitude volontaire » qui pourrait d'ailleurs rapidement devenir involontaire mais insurmontable. À l'inverse, le numérique permet d'intensifier l'incalculable de la même manière que l'écriture en Grèce Antique a eu d'immenses effets d'individuation et d'enrichissement de la diversité sociale – en particulier en rendant possible la citoyenneté, qui fut la naissance d'un nouveau processus d'individuation psychique et collective.[90]

De la même manière, les données personnelles et leur utilisation peuvent être analysées comme, à la fois, un remède et un poison par les individus. Suivant une approche rationnelle, ces derniers réalisent donc un calcul rationnel entre les avantages et les inconvénients que posent ces pratiques. Alessandro Acquisti, Curtis Taylor et Liad Wagman évoquent ce raisonnement rationnel des individus dans les termes suivants : « *The market for personal data and the market for privacy are two sides of the same coin, wherein protected data may carry benefits and costs that mirror or are dual to the costs and benefits associated with disclosed data for both data subjects and data holders* »[91]. L'idée à retenir ici est cette image d'une pièce de monnaie avec deux faces opposées. Suivant cette analogie, Grazia Cecere et Fabrice Le Guel affirment que « l'exploitation de ces ressources informationnelles par les entreprises y est présentée comme une source de bien-être pour les consommateurs, d'innovations et d'opportunités commerciales inédites, mais également de menaces sur la vie privée et d'externalités négatives pécuniaires »[92]. Au cours de l'entretien semi-directif mené, Coralie a pu affirmer à propos des entreprises : « Si ça leur permet de cibler plus précisément leurs clients, pour moi c'est un avantage. Après, il ne faut pas que ce soit intrusif. C'est vraiment la limite de l'utilisation des données personnelles. C'est sûr que ça a un côté relativement terrifiant, le fait que des marques ont accès à nos données »[93]. Des théories précédentes aux entretiens qualitatifs menés dans leur ensemble, il a été possible de mettre en lumière les éléments suivants : les individus jugent la valeur de leurs données personnelles, et donc varient leurs comportements, en fonction des risques qu'ils perçoivent. Au-delà de la

[90] LACROIX, Dominique, "Le blues du Net, par Bernard Stiegler », Blog Lois des réseaux, http://reseaux.blog.lemonde.fr/2013/09/29/blues-net-bernard-stiegler/, consulté le 07/05/16.
[91] ACQUISTI, Alessandro, CURTIS, Taylor et WAGMAN, Liad, « The Economics of Privacy », http://ssrn.com/abstract=2580411.
[92] CECERE, Grazia et LE GUEL, Fabrice, « Les modèles d'affaires sont-ils trop indiscrets ? », Réseaux, n°189, 2015, pp 77-101.
[93] Voir annexe 9

vision d'individus très peu informés des pratiques relatives à l'usage de leurs données personnelles, il est possible de mettre en avant des individus qui tiennent à leur « intimité ». La complexité de l'analyse est que cette notion d'intimité relève de nombreuses définitions par les individus eux-mêmes. Parfois, il s'agira de maintenir une vie privée, c'est-à-dire familiale par exemple, divulguée aux regards des autres (individus et organisations incluses). Pour d'autre, l'intimité est un élément qui permettrait d'assurer une sécurité forte pour soi et pour ses proches.

Suite aux éléments présentés précédemment, une partie des analyses du processus décisionnel des individus concernant la divulgation de leur vie privée a mis en avant des raisonnements rationnels de la part des individus. Suivant la notion de « *data as a commodity* », les individus sont alors considérés comme des objets économiques coopérant au partage de leurs données personnelles[94]. A partir de ce constat, le travail d'une multitude de chercheurs sur ces questions ont permis d'aboutir au constat suivant : les individus procèdent à un calcul rationnel lors de la divulgation de leurs données personnelles. Notamment pour Tamra Dinev, Heng Xu, Jeff H. Smith et Paul Hart, les individus réalisent « *an anticipatory, rational weighting of risks and benefits when confronted with the decision to disclose personal information or conduct transaction* »[95]. Cette théorie a été dénommée « *Privacy Calculus* » par Culnan et Amstrong dès 1999. Elle a ouvert la voie à de nombreuses recherches.

B) …à celle du « Social Exchange Theory »

Se rapprochant de la théorie du « *Privacy Calculus* », des chercheurs en psychologie et en sociologie ont également traité de la rationalité de l'individu face à des enjeux concernant sa vie privée. Pour Jennifer King, la « *Social Exchange Theory* » permet de mettre en lumière des comportements rationnels de la part des individus. Définie comme « *a sociological theory which describes the relationships that 'develop within structures of mutual dependances between actors'. Actors within these relationships engage in 'reoccurring mutually contingent exchanges with specific*

[94] SMITH, H. Jeff, DINEV, Tamara et XU, Heng, "Information Privacy Research: An Interdisciplinary Review", MIS Quarterly, 2011.
[95] DINEV, Tamara, XU, Heng, SMITH, H. Jeff et HART, Paul, "Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-related Concepts", European Journal of Information Systems, 2013.

partners over time »[96], cette théorie affirme que les individus agissent en fonction d'un élément clé des échanges sociaux : celui de la réciprocité. En effet, lorsqu'ils sont face à une situation de divulgation de leur vie privée, ils s'attendent à recevoir, en retour, un bien ou un service équivalent. J. King énonce ainsi « *Even when disclosures are made to companies and organizations rather than to individuals, the disclosures are acts of social exchange primed by expectations of reciprocity and relationship building* »[97]. Afin d'illustrer son propos, elle prend justement en exemple des applications mobiles de running.

> Consider a privacy-loving jogger contemplating using a new fitness app: when making the decision to provide the app with her personal information, the jogger is likely not actively calculating the disclosure in terms of benefit versus risk, or exclusively in terms of cost versus benefit, but rather how the app is going to help her achieve her fitness goals. Secondarily, she may have concerns about the use and protection of the information she provides, but her first-order evaluation is focused on how this tool can help her improve her fitness, and the disclosure may seem an appropriate exchange for the service. When the relationship between our jogger and the application provider is examined as an exchange, her decision to use the fitness app despite its potential risk to her personal information looks less paradoxical. *Considering the social elements allows us to evaluate the impact of other factors beyond the risk element and the economic value of the exchange: her motivations, the power relationship between the two parties, and the wider social context.*[98]

Au cours de l'entretien avec Coralie, il a pu être constaté une acceptation de la divulgation en échange d'un service équivalent : celui de l'application mobile Nike Running : « Sur Nike, je n'ai pas ce sentiment –là. Je n'ai pas le sentiment d'avoir diffusé mes informations à un grand nombre de partenaires ou d'acteurs »[99].

L'ensemble des précédentes théories qualifient donc les individus comme rationnels. Pour ces auteurs et chercheurs, les individus procèdent à un calcul précis entre les données qu'ils divulguent et les biens et/ou services qu'ils obtiennent en échange. Néanmoins, Ces dernières années, cette figure de l'individu rationnel a régulièrement été critiquée.

[96] KING, Jennifer, "Understanding Privacy Decision-Making Using Social Exchange Theory", 2015, https://networkedprivacy2015.files.wordpress.com/2015/02/jenking_cscw_privacy_set_2015.pdf, consulté le 21/04/16.
[97] *Ibid*.
[98] *Ibid*.
[99] Voir annexe 9

Section 2 – Vers le constat d'une irrationalité des individus

En économie, la figure de l'individu rationnel a pu être critiquée par de nombreux courants souhaitant décrire la réalité du marché. Cette critique a notamment été conduite par Herbert Alexander Simon et sa notion de « *bounded rationality* », ou de rationalité limitée. Economiste ayant reçu le prix Nobel d'économie en 1978, H. A. Simon a publié, dès 1957, une première explication de cette notion, dans son ouvrage *Models of Man: Social and Rational – Mathematical Essays on Rational Human Behavior in a Social Setting*. Il y définit la rationalité limitée comme « *the incapacity of exercise of global rationally makes the economic agents beings endowed with a bounded rationality* »[100]. Dans son ouvrage *Theories of Bounded Rationality* datant de 1972, il y présente les trois limites à la rationalité : (1) « *uncertaintly about the consequences that would follow from each alternative* », (2) « *incomplete information about the set of alternatives* » et (3) « *complexity preveniting then necessary computations from being carried out* »[101]. C'est au sein de ce cadre théorique que l'économie comportementale a été en mesure de souligner la profonde irrationalité des individus, dans un contexte de « *privacy trades-off* ».

Ainsi, à l'opposé du discours désignant l'individu comme rationnel, la théorie du « *privacy paradox* » met en évidence une irrationalité des individus et une contradiction entre la perception de leur vie privée et les comportements concernant leur divulgation. Dans l'hypothèse où les individus seraient informés des pratiques des entreprises, certaines théories démontrent cette irrationalité.

A) Le « Privacy Paradox », une théorie toujours d'actualité ?

Pour Dan Ariely, les individus sont « *predictably irrational* »[102]. Dans le cadre de l'étude de la vie privée, cela a été également le cas avec plusieurs théories mettant en avant l'irrationalité des individus concernant la divulgation de leurs données personnelles. L'un des concepts clés à étudier est celui de « *Privacy Paradox* ». Dans son article « A privacy

[100] *SIMON, Herbert A., Models of Man: Social and Rational – Mathematical Essays on Rational Human Behavior in a Social Setting, Wiley, 1957.*
[101] *SIMON, Herbert A., Theories of Bounded Rationaly, 1972.*
[102] ARIELY, Dan, *Predictably Irrational: The Hidden Forces That Shapes Our Decisions*, 2008

paradox : Social networking in the United States » publié en 2006, Susan B. Barnes, enseignante au département Communication du Rochester Institute of Technology (RIT), a pu étudier une contradiction forte entre les propos et les comportements des adolescents américains concernant l'usage de leurs données personnelles. Toujours selon Susan Barnes, « *In America, we live in a paradoxical world of privacy. On one hand, teenagers reveal their intimate thoughts and behaviors online and, on the other hand, government agencies and marketers are collecting personal data about us* »[103]. Résumé par la formule suivante par Tobias Dienlin et Sabine Trepte « *People's concern toward privacy are unrelated to the privacy behaviors* »[104], ce concept de « *Privacy Paradox* » a ouvert la voie à d'importants débats entre chercheurs à travers le monde.

Suite aux divers entretiens menés dans le cadre de ce mémoire, certains individus interrogés ont présenté des signes de persistance de ce « *Privacy Paradox* ». Prenons l'exemple de Julie C. Malgré un certain manque d'informations sur les usages précis de ses données personnelles (« on ne saura jamais vraiment à qui sont données nos informations personnelles »), Julie déclarait qu'elle avait connaissance de leur collecte et de leur traitement : « je sais qu'on prend nos données, qu'on les utilise, qu'on les revend à des marques… […] Maintenant, je ne fais plus vraiment attention. Je sais que l'on prend mes données de toute façon. ». De fait, en dépit de ces éléments d'informations, Julie C. affirmait utiliser régulièrement l'application mobile Nike Running lors de chaque course. D'un point de vue comparé avec les autres personnes interrogées, le constat qui a pu être fait a été similaire : les individus semblent relativement au courant des pratiques des entreprises relativement à leurs données personnelles mais continuent à utiliser ces applications, considérés comme « invasives »[105].

[103] BARNES, Susan B., « A Privacy Paradox: Social Networking in the United States", 2016, http://firstmonday.org/article/view/1394/1312_2, consulté le 15/01/16.
[104] DIENLIN, Tobias et TREPTE, Sabine, "Is the privacy paradox a relic of the past ? An in-depth analysis of privacy attitudes and privacy behaviors", *European Journal of Social Psychology*, 45,285-297, 2015.
[105] Voir annexe 9

B) Les trois freins à la rationalité de l'individu par l'économie comportementale et Acquisti

Dans son article intitulé « Les comportements de vie privée face au commerce électronique, une économie de la gratification immédiate », Alessandro Acquisti énonçait qu'il est « peu probable que les individus puissent agir de façon rationnelle au sens économique lorsqu'ils doivent prendre des décisions sensibles en matière de vie privée »[106]. Pour cela, il reprend la notion de « gratification immédiate » de Ted O'Donoghue et Matthew Rabin[107]. Appartenant au courant de l'économie comportementale, qui prend le contre-pied de la théorie classique concernant la rationalité de l'individu, ce concept est ainsi défini : « *people have self-control problems : We would 'like' to behave in one manner, but instead 'choose' to behave in another. In particular, we tend to pursue immediate gratification in a way that we ourselves do not appreciate in the long run* »[108]. A l'opposé donc de la théorie de l'individu rationnel, Alessandro Acquisti poursuit le travail précédent en énonçant trois freins essentiels à la rationalité de l'individu : une « information incomplète concernant tous les paramètres », « un pouvoir limité pour traiter toute l'information disponible », et « la difficulté à ne pas dévier de la logique rationnelle de maximisation de l'utilité »[109]. Une analyse plus approfondie de ces trois freins est donc nécessaire, notamment faite à la lumière des entretiens réalisés dans le cadre de cet entretien.

Tout d'abord, selon l'économie comportementale, les individus ne disposent pas d'une information complète. Pour rappel, en économie et plus précisément au sein de la théorie des jeux, il s'agit d'une situation où les participants disposent de toutes les informations disponibles sur les autres participants. Ainsi, Alessandro Acquisti cite Georges Akerlof, docteur en sciences économiques du Massachussets Institute of Technology (MIT) pour affirmer que toutes les parties prenantes ne disposent pas de la même quantité d'informations. Toujours selon lui, ces parties prenantes peuvent également être amenées à rencontrer des « incertitudes quant à certains de ses aspects importants ». Dans le cadre de la relation des

[106] ACQUISTI, Alessandro, MBO'O IDA Michèle Francine, ROCHELANDET Fabrice, « Les Comportements de vie privée face au commerce électronique. Une économie de la gratification immédiate », Réseaux 3/2011 (n°167), pp. 105-130.
[107] O'DONOGHUE, TED et RABIN, Matthew, « The economics of immediate gratification", *Journal of Behavioral Decision Making*, Volume 13, Issue 2, pp. 233-250, 2000.
[108] *Ibid*.
[109] ACQUISTI, Alessandro, MBO'O IDA Michèle Francine, ROCHELANDET Fabrice, « Les Comportements de vie privée face au commerce électronique. Une économie de la gratification immédiate », Réseaux 3/2011 (n°167), pp. 105-130.

fournisseurs de services mobiles et les utilisateurs, il est possible de démontrer que dans certaines situations actuelles, les seconds ne disposent pas de l'ensemble des informations concernant la divulgation de leurs données personnelles. Pis encore, ils ne sont pas forcément au courant des technologies de protection.

Ensuite, deuxième frein selon A. Acquisti, l'individu est-il véritablement et pleinement rationnel ? Définie comme une « incapacité à évaluer et comparer l'étendue des avantages associés aux diverses stratégies que l'individu peut choisir dans des situations sensibles en matière de vie privé »[110], la rationalité limitée est un autre facteur permettant de souligner l'irrationalité des individus. Suite à la divulgation, souhaitée ou non, par l'individu, il a pu être constaté une perte de contrôle de ses informations. Renforcée par le manque d'informations, l'individu n'est donc plus le seul maître de la divulgation de sa vie privée auprès d'un large nombre d'acteurs : organisations gouvernementales, entreprises privées… Même si les démarches sont entreprises pour s'informer, A. Acquisti constate que les coûts sont parfois trop élevés pour disposer de l'ensemble des informations nécessaires à une quelconque reprise de contrôle.

Enfin, troisième et dernier frein, il s'agit des distorsions psychologiques auxquelles sont confrontés les individus. « Actualisation hyperbolique », « sous-assurance », « problèmes d'autocontrôle », « gratification immédiate »… l'auteur souligne l'existence de nombreuses distorsions empêchant l'émergence de la figure d'un individu rationnel[111]. D'une incohérence des préférences personnelles tendant vers une actualisation hyperbolique au biais d'autocontrôle en passant par le biais d'optimisme, A. Acquisti démontre rigoureusement l'irrationalité des individus dans un contexte de divulgation de leur vie privée. Pour lui « lorsque nous devons prendre des décisions sensibles concernant notre vie privée, nous ne disposons presque jamais de toutes les données nécessaires pour faire un choix bien informé ».

Au-delà de ces vives critiques visant la figure de l'individu rationnel, l'économie comportementale a été une base de réflexion fertile à l'essor de solutions respectueuses de la vie privée des individus. A. Acquisti énonçait que « nous prenons des décisions irrationnelles, mais une information très ciblée, fournie au bon moment par cette nouvelle infrastructure

[110] ACQUISTI, Alessandro, MBO'O IDA Michèle Francine, ROCHELANDET Fabrice, « Les Comportements de vie privée face au commerce électronique. Une économie de la gratification immédiate », Réseaux 3/2011 (n°167), pp. 105-130.
[111] *Ibid*.

numérique, finira par triompher de notre irrationalité »[112]. Revenant aux applications mobiles de running, il serait donc possible de ramener les individus au centre de notre réflexion. Le mouvement Quantified Self en général et les applications mobiles en particulier ont ainsi ouvert la voie à des pratiques à la fois bénéfiques et néfastes pour les individus. Après avoir traité de ce débat, nous devons traiter des perspectives d'évolutions à court, moyen et long terme. De façon rétrospective, le web en général est une innovation qui s'est très rapidement imposée. Encore plus avec le web mobile, de nombreuses évolutions sont à venir. Les pratiques des entreprises ne sont donc pas figées et sont prochainement amenées à évoluer. Ce travail vise ainsi à ouvrir des pistes de réflexions allant dans ce sens.

[112] ACQUISTI, Alessandro, MBO'O IDA Michèle Francine, ROCHELANDET Fabrice, « Les Comportements de vie privée face au commerce électronique. Une économie de la gratification immédiate », Réseaux 3/2011 (n°167), pp. 105-130.

Partie III : La place des individus au sein du mouvement Quantified Self : entre opportunités, critiques et perspectives

Au cours des différents entretiens menés, l'un des constats qui a pu être fait a été le suivant : les personnes interrogées partagent l'idée que la vie privée en ligne n'existe pas. Pour la plupart, ils déclarent avoir conscience de l'impossibilité de vivre sans partager leurs données personnelles. La raison à cela ? S'ils souhaitaient arrêter de partager leurs données, ils ne pourraient plus utiliser les services auxquels ils ont été habitués. On pense notamment à Google ou à Facebook mais aussi aux applications mobiles. Julien B. affirmait ainsi :

> « En fait, que l'on soit favorable ou défavorable, cela n'aura pas beaucoup d'impact au final. Je m'explique. De toute façon, on ne reviendra plus en arrière. C'est tellement pratique que, oui, tu laisses une partie de tes données personnelles au service d'une utilisation qui est plus simple et plus adaptée à toi, plus ciblée et plus centrée sur tes besoins. Au final, je dirais que la vision de l'utilisateur est que tu en profites beaucoup plus que finalement ce que cela va te coûter derrière. »[113]

De façon globale, le sentiment partagé est celui d'une obligation notoire. Selon leurs propos, ils se disent au courant des pratiques de collecte et de traitement de leurs données personnelles comme de leurs usages par les entreprises.

Le constat précédent permet ainsi d'ouvrir notre réflexion en cours par une approche exploratoire. Il semble désormais nécessaire de traiter d'un important débat qui ne remonte pas à l'ère numérique : celui opposant les « techno-optimistes » aux « techno-sceptiques ». Les premiers regroupent aussi bien des auteurs que des dirigeants d'entreprise de la Silicon Valley et d'ailleurs. Pour eux, la « data-driven innovation » et le Quantified Self tendent vers une amélioration nécessaire des individus, de leurs interactions ou encore de leurs actions sur la planète. Source d'opportunités, l'adoption des nouvelles technologies est inévitable et, ainsi, doit être accompagnée. Les seconds se posent en totale contradiction avec les précédents. Leur objectif commun est de pointer du doigt les dérives du « solutionnisme de la Silicon Valley ». Ce n'est qu'après avoir traité cette opposition ancienne qu'il sera possible

[113] Voir annexe 11

d'envisager les perspectives concernant la vie privée des individus et d'aborder notamment des propositions de systèmes techniques respectueux de leurs données personnelles et, par conséquent, de leur vie privée.

Chapitre I. Une dichotomie possible des conséquences de l'usage des données personnelles sur les individus et leur vie privée

De la même manière que pour les entreprises, la captation et le traitement des données personnelles par les individus eux-mêmes ont pu être étudiées comme d'un « pharmakon ». D'un côté, les individus pourraient en tirer des bénéfices majeurs alors que de l'autre, cela conduirait à une aliénation vis-à-vis de la technique et à une « nouvelle morale hygiéniste » (E. Sadin). Dans le rapport *Rethinking personal data – A New Lens for Strengthening Trust* du World Economic Forum, ses auteurs ont pu aborder la question des applications mobiles de sport en ces termes :

> The increasing adoption of digital fitness tracking devices presents a new level of complexity and highlights the importance of context for the degree of individual control. *While there is an opportunity to combine and commingle these new intimate, high-resolution, activity-based health data with other data sets to provide a daily health dashboard for individuals, there are a range of new uncertainties on the data quality and how these combined data sets could be used for non-health related uses*[114].

Ce document met en lumière les deux facettes du mouvement Quantified Self. D'un côté, les applications mobiles de sport offrent des opportunités uniques aux individus. Mais, au-delà de cette vision dite « techno-optimiste », plusieurs critiques se sont élevées contre les usages précédemment présentés conduisant, selon leurs auteurs, à un asservissement des individus aux données.

Section 1 – De la « data driven economy » au « data driven people »

Dans son ouvrage *Pour une sociologie historique de la quantification* publié en 2008, Alain Desrosières traite de la question de la quantification comme d'un « outil de

[114] World Economic Forum, Rethinking Personal Data: A New Lens for Strengthening Trust, 2014.

gouvernement » et d'un « outil de preuve ». Selon lui, « l'hypothèse est que la quantification entendue comme l'ensemble formé de conventions socialement admises et des opérations de mesures, créé une nouvelle façon de penser, de représenter, d'exprimer le monde et d'agir en lui »[115]. La quantification conduirait vers une véritable « connaissance par les nombres ». L'illustration moderne de cette notion serait le Big Data ou la « data-driven innovation », expression issue d'un récent rapport de l'OCDE[116].

Désormais, l'expression qui revient régulièrement dans les médias mais aussi dans les rapports économiques divers est celle de « data driven economy ». Derrière ce concept clé, les données personnelles sont perçues comme centrales qu'il faut capter et analyser. L'objectif affiché est de tendre vers des pratiques optimales permis par des nouvelles méthodes de traitement des données. S'appliquant à la sphère économique, financière ou encore étatique, les données personnelles sont perçues comme des indicateurs clés. En anglais, on parle de « *Key Performances Indicators* » (ou KPI). Ces derniers conduisent à une prise de décisions reposant sur des analyses statistiques cruciales. Suivant le raisonnement précédent, le mouvement Quantified Self promeut l'idée que la captation et le traitement des données sont un moyen d'accroitre la connaissance de soi. Cette analyse permettrait ensuite de tendre vers une amélioration de ses capacités physiques voire mentales en fonction des indicateurs mis en évidence.

A) La quantification comme outil de connaissance de soi…

Avec les applications mobiles de running, et plus généralement de l'essor du « *self-tracking* », ce sont les réflexions de Michel Foucault qui ont pu être réactualisées. En effet, dans son ouvrage *L'origine de l'herméneutique de soi*, Michel Foucault énonçait le concept de « technologies de soi » qu'il définissait comme des « techniques qui permettent aux individus d'effectuer par eux-mêmes un certain nombre d'opérations sur leur propre corps, sur leur propre âme, sur leurs propres pensées, sur leur propre conduite, et cela de manière à se transformer eux-mêmes, se modifier eux-mêmes et atteindre un certain état de perfection, de bonheur, de pureté, de pouvoir surnaturel, etc. ».[117] Dans ce courant d'idées, plusieurs auteurs ont pu analyser le mouvement de « self-tracking » par les applications mobiles, et notamment

[115] Alain Desrosières, Pour une sociologie historique de la quantification, Presse de l'école des Mines, 2008.
[116] OECD, « Data-driven Innovation for Growth and Well-being", http://oe.cd/bigdata, consulté le 01/05/16.
[117] FOUCAULT, Michel, L'origine de l'herméneutique de soi. Conférences prononcées à Dartmouth College [1980], Vrin, 2013, p.53

celles de course à pied, comme des technologies de soi au sens foucaldien. Pour Fabien Granjon, Véra Nikolski et Anne-Sylvie Pharabob, le self-tracking s'apparente à « une émergence d'une nouvelle forme de culture de soi, une nouvelle *techné tou biou*, prescrivant la nécessité de 'prendre soin de soi-même' ». Ainsi, le mouvement Quantified Self se définirait comme une « objectivisation chiffrée de réalités existentielles qui leur sont propres »[118].

Dans le même ordre d'idée, le philosophe français Eric Sadin traite également de cette question du « self-tracking » et du Quantified Self dans son ouvrage *La vie algorithmique, critiques de la raison numérique.* Il y énonce notamment :

> Finalement, le Quantified Self, à l'écart du principe de la seule mesure de soi et du 'souci assisté de soi' doit être entendu comme constituant l'une des bases, une des strates fondamentales présentes et à venir, conditionnant l'éditification d'une cartographie détaillée, globale et évolutive des états du monde. C'est dans cette littéralité que le terme doit être saisi dans sa pleine puissance de vérité, concourant à soutenir une quantification toujours plus intégrale des êtres, produisant comme effet collatéral de participer pour une large part à la consolidation et au perfectionnement continus d'un Quantified World.[119]

A partir de cette « cartographie détaillée » et de ce « *Quantified World* », les individus ont l'opportunité d'améliorer leurs pratiques quotidiennes et de tendre vers un « soi amélioré ». La mesure de soi viserait ainsi à « objectiver certains faits tenants à leur 'moi' et brouillés par leur subjectivité »[120]. Deuxième temps fondamental du Quantified Self, il s'agit également de la principale motivation des individus interrogés. En effet, leur utilisation respective des applications mobiles telles que Nike Running ou Runstatic est motivée tant par une volonté de suivi de leurs performances mais aussi d'amélioration de ces dernières dans le temps long.

[118] GRANJON, Fabien, NIKOLSKI, Véra et PHARABOD, Anne-Sylvie « Métriques de soi et Self-tracking. Une nouvelle culture de soi à l'ère numérique et de la modernité réflexive ? », Recherches en communication, n°35, 2011.
[119] SADIN, Eric, La vie algorithmique, critiques de la raison numérique, Editions L'échappée, 2015.
[120] GRANJON, Fabien, NIKOLSKI, Véra et PHARABOD, Anne-Sylvie « Métriques de soi et Self-tracking. Une nouvelle culture de soi à l'ère numérique et de la modernité réflexive ? », Recherches en communication, n°35, 2011.

B) …permettant une potentielle amélioration de soi

Pour J. Heath et J. Anderson, les individus ont recours à des stratégies multiples pour avoir accès à des informations précises et véridiques à propos d'eux-mêmes afin, *in fine*, d'accroitre le contrôle de leur personne et ainsi devenir plus efficace dans l'accomplissement de leurs tâches au quotidien[121]. Quant à lui, Eric Sadin affirme qu'il est désormais possible de : « participer à une bonne préservation de la santé, grâce à une manifestation objectivée d'une partie de soi par les nombres ». Il poursuit en décrivant les technologies de Quantified Self, applications mobiles incluses, comme des « systèmes qui non seulement exposes les données brutes, mais qui se présentent sous la forme de 'coachs numériques' qui délivrent des synthèses d'après des bases multicritères, signalent toute progression ou recul des performances, et suggèrent des feuilles de routes personnalisées suivant les circonstances ». Suivant une idée similaire, Melanie Swan a parlé de l'émergence d'un « *extended connected self* ». Selon elle, la combinaison de la « quantification par la donnée et le 'self-tracking' permettent des capacités qui n'étaient pas possibles avec les sens ordinaires »[122]. Au travers de ces différentes réflexions, l'idée d'une subjectivisation du rapport au corps a pu donc être soulevée. Cette dernière a été renforcée par l'essor de technologies ayant de fortes capacités de stockage et de calcul des données. Désormais, les individus se perçoivent à travers les appareils de mesure et des données qu'ils fournissent.

Pour Evgeny Morozov, dans son ouvrage *Le mirage numérique, pour une politique du Big Data*, la tendance mise en avant précédemment peut être qualifiée de « dividende de la surveillance ». Il explique, en effet, que « l'internet des objets, le Big Data et le bouleversement de l'ensemble de l'univers par une poignée de start-up californienne apporteront l'abondance économique, l'émancipation politique et la prospérité générale »[123]. Après avoir présenté plusieurs exemples des bienfaits de plusieurs applications illustrant la « physique sociale » du chercheur américain Alex Pentland, E. Morozov pointe du doigt les dérives de la Silicon Valley. Au sein du dernier paragraphe de son troisième chapitre, il énonce que :

[121] HEATH, Joseph et ANDERSON, Joel, "Procrastination and the extended will" in C. Andreou & M. D. White, *The Thief of time*, Oxford University Press, 2010.
[122] SWAN, Melanie, "The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery", 2013.
[123] MOROZOV, Evgeny, Le mirage numérique. Pour une politique du Big Data, Editions Les Prairies Ordinaires, ,2015.

> Notre époque est marquée par une profonde *asymétrie épistémique*. A l'hyper-visibilité du citoyen individuel – que l'on peut suivre à la trace, au moyen de toutes sortes d'appareils intelligents – correspond l'hyper-invisibilité croissant de tous les acteurs. […] Les entreprises sèment la confusion sur l'impact réel de leurs activités, elles fabriquent de l'ignorance en finançant des études pseudo-scientifiques qui les arrangent. Wall Street produit en série des instruments financiers si opaques qu'ils découragent tout effort de compréhension.[124]

E. Morozov a ainsi pu être qualifié de « techno-sceptique ». Derrière ce courant hétérogène, de nombreux auteurs ont pu élever leur voix contre ce qu'appelle E. Morozov un « solutionnisme » de la Silicon Valley. Pointant du doigt le Big Data dans son ensemble et notamment le mouvement Quantified Self, ces précédents auteurs ont soulevé la question de la perte de contrôle de la vie privée des individus. A ce niveau de la réflexion, il semble donc nécessaire d'approfondir ces critiques avant d'aborder les perspectives à court, moyen et long terme.

Section 2 – Une perte de contrôle de la vie privée des individus

L'essor croissant des algorithmes au sein de la vie quotidienne des individus a suscité des réactions de la part des chercheurs en science de l'information et de la communication mais aussi des responsables politiques et des individus dans toute leur diversité. Avec des ouvrages comme *A quoi rêvent les algorithmes ?* de Dominique Cardon[125] par exemple, une double critique a été formulée. D'une part, ces nouveaux systèmes techniques sont fondamentalement opaques, de leur conception à leur utilisation par les organisations. D'autre part, et découlant de la précédente, une perte de contrôle des individus sur leur vie privée a été pointée du doigt.

A) Un système au fonctionnement opaque

Dans son ouvrage *The Black Box Society, The Secret Algorithms That Controls Money and Information*, Frank Pasquale évoque le concept de « *black box* » afin de qualifier ces nouveaux systèmes techniques :

[124] *Ibid*.
[125] CARDON, Dominique, *A quoi rêvent les algorithmes ?*, La République des idées, 2015.

> The term 'black box' is a useful metaphor for doing so, given its own dual meaning. It can refer to a recording device, like the data-monitoring systems in planes, trains and cars. Or It can mean a system whose workings are mysterious; we can observe its inputs and outputs, but we cannot tell how one becomes the other. We face these two meanings daily: tracked ever more closely by firms and government, *we have no clear ideal of just how far much of this information can travel, how it is used, or its consequences*.[126]

Ainsi, le Big Data peut être représenté comme une boîte noire ayant une double nature : un appareil de mesure de l'ensemble des informations (similaires aux boîtes noires présentent dans les avions par exemple) et un système dont on ne connaît pas les rouages précis. Dans le cas du mouvement Quantified Self, il est possible de reprendre ce concept de « Black box » afin de mettre en avant le manque d'informations transmis par les fournisseurs de service tant sur les moyens de captation des données personnelles que sur la nature des données ou encore du moment de cette captation. Pour une majorité des personnes interrogées, le constat est sensiblement le même : le fonctionnement des applications mobiles de running relatif à l'usage des données personnelles est opaque.

Au final, quelles conséquences de cette opacité peuvent-elles être mises en avant ? Selon le rapport « La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information » présenté au Sénat, « l'opacité des systèmes d'information conduit ainsi à une méfiance générale des individus, qu'accompagne une tendance générale au conformisme et au mimétisme social »[127]. Ce même rapport évoque les travaux des professeurs Yves Poullet et Antoinette Rouvroy : « l'opacité des systèmes et l'information déficiente procurée aux citoyens conduit ces derniers à s'imposer des restrictions et à s'autocensurer, par crainte d'adopter des comportements qui seraient considérés comme étranges par des tiers »[128]. Plus qu'une autocensure, certains auteurs ont parlé d'une véritable perte de contrôle des individus sur leur vie privée.

[126] PASQUALE, Frank, The Black Box Society, The Secret Algorithms That Controls Money and Information, Harvard University Press, 2015

[127] DETRAIGNE, Yves et ESCOFFIER, Anne-Marie, Rapport d'information fait au nom de la commission des lois, « La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information », n°441, 2009.

[128] *Ibid*.

B) Vers une perte de contrôle de la vie privée des individus ?

Au-delà du fonctionnement opaque des systèmes techniques, les utilisateurs sont confrontés à des pratiques peu respectueuses de leurs données personnelles et de leur vie privée. Selon Marjolein Lanzing, « *the notion of 'self-tracking' is somewhat misleading. Although self-tracking appears to merely entail self-surveillance, it also involves co-veillance and surveillance. Sharing one's data with peers is encouraged and producers of self-tracking devices often track what these devices are recording by default. Morever, the data produced by self-tracking is increasingly shared and used its usual contexts.* »[129] Ces pratiques, que nous avons traitées précédemment, ont potentiellement tendu vers une perte de contrôle des individus de leur vie privée voire de ce qui a été appelé vers un « *disempowerment* » des individus. N'ayant pas un niveau d'information élevé ni un contrôle relatif de leurs données personnelles, la majorité des utilisateurs de ces services voient leur vie privée se réduire. Pour certains auteurs, dont Frank Pasquale, il est nécessaire de tendre non seulement vers une transparence des systèmes mais aussi vers une régulation des pratiques des organisations du point de vue de la captation et du traitement des données personnelles.

Au sein de l'article intitulé « Lifelogging is dead (for now) » publié sur le site web spécialisé ComputerWorld, l'un des instigateurs du mouvement Quantified Self proclamait la mort de la pratique du « lifelogging ». En effet, pour l'ingénieur et le chercheur du laboratoire Microsoft Research Gordon Bell, l'expérience d'auto-mesure de soi appelée MyLifeBits Project débutée au cours de l'année 2000 « n'a pas été quelque chose qui m'a beaucoup apporté dans la vie ». Au cours de l'interview menée par le journaliste Mike Elgan, il poursuit en déclarant que « le smartphone est la nouvelle version du Memex de Bush »[130]. Faisant référence aux travaux de Vannevar Bush qui, en 1945, anticipait l'émergence du Memex, « une sorte de bureau qui pourrait instantanément tout enregistrer, transmettre et retrouver, d'infimes brides d'informations à des livres dans leur intégralité »[131]. Ce constat de l'échec du Quantified Self, également souligné par Chris Anderson le 16 avril de la même année, repose

[129] LANZING, Marjolein, The Self Transparent, Ethics and Information Technology, Volume 18, Issue 1, pp 9-16, March 2016, DOI: 10.1007/s10676-016-9396-y

[130] ELGAN, Mike, "Lifelogging is dead (for now)", www.computerworld.com/article/304897/personal-technology/lifelogging-is-dead-for-now.html, consulté le 15/05/16.

[131] BUSH, Vannevar, "As We May Think", *Atlantic Monthly*, 1945.

notamment sur l'observation suivante : « *More data is being generated than ever before, but it's hard to bring it all together and hardly anybody wants to* »[132].

Au-delà de ces anticipations par les porte-paroles même du mouvement Quantified Self, ce mémoire a permis de souligner une asymétrie majeure entre les entreprises collectant et traitant les données personnelles et les utilisateurs de leurs services. Pour certains auteurs, ils existent des alternatives possibles permettant de rééquilibrer la relation qui s'est installée ces dernières années afin, notamment, de redonner le pouvoir aux individus. Selon eux, cet « *empowerment* » des individus passe par une reprise du contrôle des utilisateurs de leurs données personnelles et de leur vie privée.

Chapitre II. La reprise de contrôle des données personnelles par les individus

Ces dernières années, de nombreuses voix se sont élevées afin de remettre les individus au centre des réflexions sur la question de la vie privée. S'opposant à des systèmes opaques et peu respectueux des données personnelles des individus, plusieurs initiatives ont pu émerger. Dans le cadre de ce mémoire, deux voies doivent être abordées. La première vise à repenser les relations entre les firmes et les individus et a pu être qualifiée de « *top-down* ». La seconde est, à l'inverse, de type « *bottom-up* » et vise à permettre aux individus de reprendre le contrôle de leurs données. L'objectif commun de ces deux voies est de tendre véritablement vers un « *empowerment* » des individus. Derrière ce concept, il est possible de souligner une volonté de lutter conjointement contre les freins à la rationalité des individus : le manque d'information, le manque de contrôle et les diverses distorsions psychologiques des individus.

Comme première illustration, le « *privacy nudging* » s'inscrit plutôt dans cette voie, visant à refonder la logique « *top-down* ». Partant des développeurs et de la phase de conception même des services, le « *privacy nudging* » vise à inciter les individus à une prise de conscience de la valeur de leurs données personnelles. Cela passe notamment par la réduction des biais cognitifs des individus. D'autre part, le « *Personal Data Management* »

[132] ELGAN, Mike, "Lifelogging is dead (for now)", www.computerworld.com/article/304897/personal-technology/lifelogging-is-dead-for-now.html, consulté le 15/05/16.

est un concept visant à redonner le contrôle des données personnelles aux individus grâce à l'émergence de nouvelles plateformes. Ces deux voies, issues de deux visions différentes, offrent la possibilité d'analyser deux alternatives possibles aux modèles actuels.

Section 1 – Le « Privacy nudging » comme moyen de sensibiliser les individus aux questions de leur vie privée.

Pouvant être qualifiée d'approche « *top-down* », la première voie vise à inciter les fournisseurs de services à créer des sites web ou des applications mobiles respectueux de la vie privée de leurs utilisateurs dès la phase de conception. Ces dernières années, le concept de « *Privacy by Design* », pouvant être traduit par « protection intégrée de la vie privée », a notamment alimenté les réflexions autour de cette approche. Il a été développé par le Commissaire à l'information et à la protection de la vie privée de l'Ontaria (Canada) Ann Cavoukian dans les années 1990. Il vise à « incorporer des règles de protection des données personnelles et de la vie privée dans les dispositifs informatiques utilisés par les individus, dès la conception de ces dispositifs »[133]. Ce concept préventif est une approche qualifiée de « volontariste très marquée, louable par son désir de prendre ces problèmes à bras-le-corps, en proposant un changement d'orientation de la régulation, mais investissant la technologie d'un rôle qu'elle ne peut assumer seule »[134]. Dans le même courant d'idées, plusieurs auteurs ont énoncé l'idée de créer des dispositifs techniques incitant leurs utilisateurs à prendre en compte leurs données personnelles. Ce fut le cas avec les « *nudges* » ou coups de pouce.

A) Qu'appelle-t-on les « nudges » ?

Popularisés par l'économiste Richard Thaler et Cass Sunstein, professeur à Harvard, les « *nudges* » s'opposent à la vision évoquée précédemment de l' « homo economicus ». Appartenant au courant de l'économie comportementale, ces deux auteurs évoquèrent l'idée d'un « paternalisme libertarien ». Dans leur ouvrage, ils ont pu définir cette notion ainsi : « *A*

[133] Privacy by design
https://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf
[134] RALLET, Alain, ROCHELANDET, Fabrice et ZOLYNSKI, Célia, « De la Privacy by Design à la Privacy by Using », revue Réseaux, n°189, 2015/1.

nudge, as we will use the term, is any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid »[135]. Cette mise en scène des choix (ou « *Choice architecture* ») se présente ainsi sous la forme d'une organisation du contexte de prise de décisions des individus. La particularité émise par Thaler et Sunstein est qu'il n'est pas neutre, mais oriente à l'aide d'un « coup de pouce » les décisions des individus.

Le professeur de philosophie Frédéric Orobon énonce que « de tels dispositifs peuvent être perçus comme n'étant rien d'autre qu'une manipulation symétrique à celles que les publicitaires utilisent pour nous faire acheter des produits dont nous n'avons pas réellement besoin. A cette objection, C.R. Sunstein et R.H. Thaler répondent que les coups de pouce n'annulent pas la liberté de choix, et qu'il s'agit d'une influence en vue d'un bien que l'individu aurait finalement choisi s'il n'avait pas été aveuglé par différents biais. En ce sens, la fin justifie les moyens »[136]. La dernière partie de cette citation est intéressante à souligner car elle renvoie justement aux freins évoqués précédemment visant la figure de l'individu rationnel. En cela, il s'agirait moins de manipulation que d'une méthode permettant de corriger le manque d'informations des individus ou encore leurs distorsions psychologiques.

B) Une application possible des « nudges » dans le domaine de la vie privée

Dans leur ouvrage cité précédemment, R.H. Thaler et C.R. Sunstein ont donné une pluralité d'exemples, allant de la construction des magasins à la réduction de la consommation d'énergie en passant par un moyen de remédier à l'épargne insuffisante des Américains. Pour un ensemble de chercheurs, l'utilisation des nudges ne s'arrête pas au champ politique mais peut potentiellement corriger les dérives concernant l'usage des données personnelles des utilisateurs des applications mobiles et les différentes atteintes à leur vie privée. Cette vision a pu être, tout d'abord, développée dans l'article intitulé « *Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging* ». De façon collégiale, les auteurs de cet article publié en 2015 ont soulevé l'idée que des « privacy nudges » pouvaient être introduites au sein même de la conception des applications mobiles

[135] THALER, Richard H. et SUNSTEIN, Cass. R., *Nudge, la méthode douce pour inspirer la bonne décision*, Broché, 2010.
[136] OROBON, Frédéric, « Le paternalisme libéral, oxymore ou avenir de l'Etat-Providence », revue *Esprit*, 2013/7.

afin de « *make privacy risks more salient and help users move towards privacy settings that better align with their privacy expectations and concerns* »[137]. Ces coups de pouce répondraient ainsi au manque de visibilité des individus concernant la captation et le traitement de leurs données personnelles par des entreprises tiers qui a pu être mis en avant au cours de ce mémoire. Selon eux, *« in the mobile context, the potential for nudges to support privacy decision making is appealing. It may include notifications that, in contrast to traditional notices, highlight the recipients, contexts, or type of personal information being shared via a mobile device* »[138]. Les différents dispositifs proposés permettront ainsi d'alerter plus efficacement les individus et de remplacer les anciennes pratiques qui, nous l'avons montré, ne fonctionnent pas dans la majorité des cas.

Dans un article co-rédigé par des chercheurs du laboratoire Microsoft Research et de l'université de Washington, ce « *privacy nudging* » passe par la création de représentations visuelles indiquant aux mobinautes si une application mobile est respectueuse de la vie privée de ses utilisateurs, en amont de son téléchargement. A la manière d'un système d'évaluation, ce « *Visual Framing* » vise donc à sensibiliser les individus aux questions du respect de leurs données personnelles. Les coups de pouce concernant le respect de la vie privée peuvent également s'implanter après le téléchargement des applications mobiles[139]. Dans un autre article portant sur cette question, les auteurs ont pu soulever l'hypothèse de la création de « *Personalized Privacy Assistants* ». Ces derniers ont pu être définis de la manière suivante : « *the personalized privacy assistants leverage the apps a user has installed on his or her mobile phone to elicit their privacy preferences and offer recommendations on how to configure associated permission settings, including options to automatically configure multiple permission settings at once* ». Ces dispositifs conduiraient, ici encore, les individus à avoir une visibilité renforcée sur les permissions qu'ils ont accordé aux diverses applications

[137] ALMUIMEDI, Hazim, SCHAUB, Florian, SADEH, Norman, ADJERID, Idris, ACQUISTI, Alessandro, GLUCK, Joshua, FAITH CRANOR, Lorrie et AGARWAL, Yuvraj, « Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI'15). New York, 2015.

[138] *Ibid*.

[139] CHOE, Eun Kyoung, JUNG, Jaeyeon, LEE, Bongshin et FISHER, Kristie, « Nudging People Away From Privacy-Invasive Mobile Apps Through Visual Framing », *Human-Computer Interaction*, Volume 8119 of the series Lectures Notes in Computer Sciences, 2013, pp 74-91.

installées sur leurs appareils. L'objectif affiché est de « conduire à des changements de permissions plus restrictives sans sacrifier le confort d'utilisation par les individus »[140].

A ce niveau de la réflexion, il doit être noté que les « *nudges* » sont également utilisés par les entreprises lors de leurs actions marketing. Ryan Calo a notamment cherché à répondre à la question suivante : à partir de quel moment la personnalisation devient un problème pour la protection du consommateur ? La notion de « *Market Manipulation* » renvoie à l'utilisation de « nudges » par les entreprises : « *companies and other firms will use what they know about human psychology to set prices, draft contracts, minimize perceptions of danger or risk, and otherwise attempt to extract as much rent as possible from their consumers* ». Les « coups de pouce » ne sont donc pas forcément efficaces car les individus sont soumis à ce genre de pratiques quotidiennement, et notamment dans le cadre du marketing moderne[141].

Section 2 – Essor des plateformes de gestion des données personnelles

Des voies alternatives ont pu être tracées ces dernières années avec pour objectif de replacer les individus au centre du processus de divulgation de leurs données personnelles. L'expression « *Personal data empowerment* » a ainsi pu voir le jour. Au sein du rapport « Personal data empowerment, time for a fairer data deal », le Citizens Advice Bureau définit ce concept par les propos suivants : « *consumers having meaningful control over the use of their personal data, and being easily able to understand and determine how it is used and the benefits they will derive, all within appropriate trust mechanisms* »[142]. Derrière cette définition, que l'on pourrait traduire par « émancipation par la donnée », le principe prôné est celui de donner aux individus les outils nécessaires à la captation, à la manipulation et à l'utilisation de leurs propres données personnelles pour leur permettre, *in fine*, d'en tirer des

[140] LIU, Bin, ANDERSEN, Mads Schaarup, SCHAUB, Florian, ALMUHIMEDI, Hazim, SADZH, Norman, AGARWAL, Yuvraj et ACQUISTI, Alessandro,"To Deny or Not to Deny: A Personalized Privacy Assistant for Mobile Apps Permission", draft version, https://www.ftc.gov/system/files/documents/public_events/776191/nsadeh_paper.pdf, consulté le 20/05/16.

[141] CALO, Ryan, "Digital Market Manipulation", 82 George Washington Law Review 995 (2014); University of Washington School of Law Research Paper no. 2013-27.

[142] Citizens Advice Bureau, Rapport "Personal data empowerment, time for a fairer data deal", 2015.

bénéfices de façon autonome. Entre concepts théoriques et enjeux spécifiques pour les individus, comment le Personal Data Management a-t-il été conceptualisé par ses créateurs ?

A) Personal Data management, quelques exemples

Dès 2013, Jacques BUS et M-H Nguyen évoquaient la notion de « *Context-aware Personal Data Management* », qu'ils ont pu définir ainsi :

> Context-Aware PDM (CPDM) enables an individual to *control the access and use of her personal data in a way that gives her sufficient autonomy to determine, maintain and develop her identity as an individual*, which includes presenting aspects (attributes) of her identity depedent on the context of the transactions (communication, data sharing, etc.) and enabling considerations of constraints relevant to personal preferences, cultural, social and leval norms.[143]

A travers cette notion, les deux auteurs ont tenté de constituer une nouvelle approche de la gestion des données personnelles à travers un écosystème décentralisé et géré par ces données personnelles. Il s'oppose notamment à la situation précédemment décrite tant du point de vue de la captation que du traitement des données personnelles. L'objectif est bien la mise en place de pratiques relatives aux données personnelles reposant sur la confiance.

De façon similaire, le chercheur anglais Reuben Binns évoque l'émergence de « Personal Information Management Services » (ou PIMS) qui marquerait l'essor d'un « *market for data-driven services, created for and controlled by individuals, centred around their needs and desires* »[144]. Toujours selon R. Binns, le « Personal Data Management » est rendu possible grâce à ce qu'il appelle des « magasins de données personnelles » (ou PDS pour « Personal Data Stores »). Ces derniers, plus qu'un espace de stockage personnel, se présentent sous la forme d'une plateforme qui centraliserait, organiserait et catégoriserait l'ensemble des données personnelles des individus issues de diverses sources externes. A terme, cette plateforme vise à offrir de nouveaux services. Il cite comme exemple les « *decision support services* » (ou « DSS »). Grâce à leurs données, les individus pourraient se

[143] BUS, Jacques and NGUYEN, M.-H. Carolyn, "Personal Data Management – A Structured Discussion", Digital Enlightenment Forum, Microsoft, 2013.
[144] BINNS, Reuben, "Personal Data Empowerment and the Ideal Observer", Faculty of Business and Law/Department of Electronics and Computer Science, University of Southampton

référer aux « DSS » pour procéder à des achats appropriés par exemple. A ces yeux, le PIMS permettrai aux individus de tendre vers l'idéal de « l'homo economicus ».

Dans cette logique d'« empowerment » des individus grâce aux données personnelles, un véritable courant de pensée a vu le jour afin de permettre la reprise de contrôle des individus de leurs données personnelles et, ainsi, de leur vie privée. Une multitude de services ont pu apparaitre avec le même but : permettre cette reprise de contrôle. Selon le rapport de Citizens Advices, le « Personal data empowerment » passe par une pluralité de services : assurer une plus grande transparence, assurer un accès à ses données personnelles, permettre l'auto-production de ses données, pouvoir stocker et gérer ses données, fournir son identité digitale, permettre l'agrégation de ses données, leur combinaison, leur contrôle, leur partage, ou encore leur monétisation.

B) « Empowerment » : entre auto-production des données et monétisation

Par souci de temps et de concision, nous nous attacherons à ne traiter que de deux points centraux de la reprise de contrôle des données personnelles par les individus : l'auto-production de ses données et la monétisation. D'une part, cette reprise de contrôle passe par la capacité des individus à capter leurs données personnelles. Comme énoncé précédemment avec le mouvement Quantified Self, il s'agit de donner aux individus les bons outils afin qu'ils puissent, par eux-mêmes, collecter une pluralité de données sur leur vie quotidienne. Avec l'exemple des applications mobiles de running, nous avons pu constater que cette auto-mesure de soi était contrebalancée par une captation des données personnelles par des acteurs tiers : entreprises en charge de ces applications, « data brokers », etc. En cela, *l'empowerment* des individus doit nécessairement tendre vers la restauration de la confiance des individus concernant ces services et les pratiques relatives à leurs données personnelles.

Au-delà de l'auto-mesure de soi, cette émancipation par la donnée a aussi été abordée du point de vue de la création de la valeur par les individus eux-mêmes. Il s'agit ici d'une véritable monétisation des données personnelles par les individus eux-mêmes au sein de « *Personal Data Stores* ». Pour Mireille Hildebrandt, cette monétisation tendrait vers un « *system of checks and balances that is constitutive for the Rule of Law, thus in a way*

reinventing the Rule of Law in the era of Big Data »[145]. Ainsi, loin du rapport asymétrique décrit précédemment, la revente des données personnelles des individus par ces derniers entrainerait un rééquilibrage des rapports de force. Comme illustration de cette démarche, il est possible de citer la plateforme Datacoup, « *the world's first personal data marketplace* ». Cette startup propose aux individus de monétiser directement leurs données personnelles en provenance de leurs comptes sociaux ou encore de leurs comptes bancaires. Les utilisateurs peuvent espérer gagner dix dollars par mois. Au sein du livre blanc « The Case for Personal Information Empowerment : the rise of the personal data store » de l'entreprise Mydex, ce type de plateformes est qualifié de « Personal Data Stores » et sont des plateformes qui permettent aux individus de rassembler, de centraliser, d'utiliser et de partager leurs données personnelles[146].

Cette question de la monétisation permet également d'en venir à une autre question subsidiaire à notre propos : les individus sont-ils prêts à payer pour acquérir des garanties concernant le respect de leur vie privée ? Pour Sarah Butler et Garrett Glasgow, les méthodes de sondages permettent de mesurer la valeur que les individus attribuent à leurs données personnelles[147]. Le chercheur italien Jacopo Staiano de l'Université de Trento a interrogé 60 utilisateurs de smartphones. Il a été constaté que, d'une part, les individus attribuent une valeur variable selon le type de données personnelles. Le constat des chercheurs a été le suivant : « *we found that location is the most valued category of personally identifiable information* ». Comme énoncé précédemment, les entretiens menés dans le cadre de ce mémoire ont également pu mettre en lumière cette variation des perceptions de la valeur. Outre cette variation en fonction du type de donnée personnelle, le contexte est également un facteur déterminant aux yeux des individus. Cette question a également été traitée par les chercheurs en économie comportementale, dont Acquisti et Grossklags. Pour Sarah Spikermann, Jana Korunovska et Christine Bauer, à partir du moment où les individus

[145] HILDEBRANDT, Mireille, « Slaves to Big Data. Or Are we?", Idp de revista de Internet, Derecho y Politica (forthcoming 2013), https://works.bepress.com/mireille_hildebrandt/52, consulté le 12/05/16.
[146] Mydex, « The Case for Personal Information Empowerment: The rise of the personal data store", https://mydex.org, consulté le 13/05/16.
[147] BUTLER, Sarah et GLASGOW, Garrett, « The Value of Personal Information to Consumers of Online Services: Evidence from a Discrete Choice Experiment", www.nera.com/publications/archive/2014/the-value-of-personal-information-to-consumers-of-online-services.html, 2014.

prennent conscience de la captation et du traitement de leurs données personnelle, la perception de leur valeur augmente de façon significative[148].

A la suite d'une étude menée sur cette question par l'opérateur téléphonique Orange, Declan Lonergan, Vice président de 451 Research, déclarait que : « *It's apparent from this research that consumers' attitude to sharing their personal data is developing rapidly as they become increasingly familiar with the concept* ». De plus, il affirmait également que « *Establishing and maintaining the necessary consumer trust to enable organisations to reap the benefits of transferring, storing and analyzing this data will become a critical new battleground for all digital players in the coming years* ». Cette question de la confiance des individus est donc intrinsèquement liée aux questions de sensibilisation et de formation des individus sur l'usage de leurs données personnelles.

[148] SPIKERMANN, Sarah, KORUNOVSKA, Jana et BAUER, Christine, « Psychology of Ownership and Asset Defense: Why People Value Their Personal Information Beyond Privacy", 2012.

Conclusion

Avec l'essor des smartphones comme des appareils de lecture (ou *devices*) ayant une forte mobilité et une forte interopérabilité, les usages des individus ont profondément évolué. En effet, ces derniers ont adopté une nouvelle forme de consommation du web. Cette extension du web mobile a été accompagnée d'une multiplication des applications, c'est-à-dire des logiciels venant ajouter des fonctionnalités aux « téléphones intelligents ». Pour la plupart, elles répondent à un besoin spécifique. Pour d'autres, elles couvrent les besoins d'une activité dans son ensemble. Ce mémoire s'est attaché à analyser les comportements des individus concernant l'utilisation d'un type d'applications spécifiques : les applications mobiles de course à pied. De Nike Running à Runstatic en passant par Runkeeper ou encore Strava, ces applications ont accompagné la progression d'une pratique sportive accessible et économique : la course à pied en extérieur. Elles offrent de nombreux avantages pour ses utilisateurs : facilité d'utilisation, suivi des performances, programmes de remise en forme ou d'entrainements réguliers et, pour la plupart, gratuité. Ce dernier point a été le véritable point de départ de notre réflexion.

En économie, la question de la gratuité a pu être largement étudiée. Nous avons notamment eu l'occasion de citer les travaux de Chris Anderson sur ce point. Au sein de la sphère numérique, cette question n'est pas nouvelle car elle remonte aux temps initiaux de la création d'internet. Anciennement, les « hackers » avaient une culture de la gratuité. Au-delà de ses fondateurs, le web a, par la suite, développé des services gratuits pour les internautes. Afin de financer leurs activités, les fournisseurs de service se sont alors tournés vers de nouvelles sources de financement. Nous avons pu citer le cas de la publicité mais aussi, et c'était le cœur de ce travail, celui des données personnelles.

Bien qu'en apparence les services proposés soient gratuits, le web a vu se développer des modèles d'affaires reposant sur les données de leurs utilisateurs. Suivant la fameuse expression, « si c'est gratuit, vous êtes le produit », ces modèles d'affaires comprennent trois types d'acteurs évoqués tout au long de ce mémoire avec, tout d'abord, les entreprises qui fournissent le ou les services, ensuite, les utilisateurs-individus et, enfin, les « *data brokers* ». Ces derniers ont pu être décrits comme des entreprises-intermédiaires spécialisées dans

l'achat et la revente des données personnelles. Avec le développement des applications mobiles, ce type de modèles d'affaires a été repris et a même connu des avancées majeures grâce, en partie, aux nouvelles données récoltées par les smartphones et leurs capteurs intégrées. Plus qu'une explosion du nombre de données personnelles collectées, elles sont également devenues toujours plus denses et plus précises : identité des utilisateurs, numéro de téléphone, géolocalisation, etc.

Au sein du mouvement Quantified Self, les applications mobiles de running ont donc permis aux entreprises qui fournissent les services d'accéder à un grand nombre de données personnelles de leurs utilisateurs. Après captation et traitement, ces données personnelles ont pu acquérir une certaine valeur jusqu'à devenir un véritable « actif stratégique » pour les entreprises. Néanmoins, du point de vue des utilisateurs, ces diverses utilisations de leurs données personnelles nous ont conduits à aborder la question de leur vie privée et, plus précisément, du respect de leur vie privée en ligne. A cette occasion, il nous a été possible d'analyser tant la perception que le processus décisionnel des individus vis-à-vis de la divulgation d'une partie de leur vie privée à des entreprises tierces. Suivant les théories précédemment évoquées par un grand nombre de chercheurs, nous avons pu traiter de deux présupposés opposés. D'une part, les individus ont pu être qualifiés d'êtres rationnels, au sens que lui donnait l'économie classique. Face à un « *pharmakon* » des données personnelles, les individus se sont attachés à opter pour le choix qui leur apporteraient le plus de bénéfices et, à l'inverse, le moins d'inconvénients dans leur vie quotidienne. De l'autre, il a été mis en lumière la figure de l'individu irrationnel. Suivant notamment l'économie comportementale, nous avons pu voir que les individus ne pouvaient pas être vus comme rationnels en raison de trois éléments cruciaux : une information incomplète, le manque de contrôle, et les biais psychologiques des individus.

Cette réflexion nous a alors conduit à replacer les individus au centre de notre analyse. Ces dernières années, un important débat s'est développé opposant, d'un côté, les individus ayant une vision favorable de l'utilisation des données personnelles et, de l'autre, des individus qualifiés de « techno-sceptiques » qui mettent en avant une pluralité de critiques : un système opaque, une atteinte à la vie privée des individus… Pour ces derniers, la captation et l'utilisation des données personnelles conduiraient à une perte de contrôle des individus de leur propre vie privée. Ainsi, dans une optique de reprise de contrôle, nous avons pu

finalement évoqués des alternatives visant à remettre les individus au centre de la réflexion. Du « *privacy nudging* » aux plateformes de « *Personal Data Management* », nous avons eu l'occasion d'aborder des approches plus respectueuses de la vie privée des individus.

A l'heure actuelle, et notamment selon Reuben Binns, ces dernières plateformes de « Personal Data Management » doivent faire face à des enjeux persistants. En effet, elles reposent sur le concept de « *marketplace* », c'est-à-dire où les individus y mettraient en vente leurs données personnelles directement. L'idée sous-jacente est que ces plateformes reposeraient sur la théorie de la « main invisible » d'Adam Smith. En théorie donc, bien que chaque individu vise leurs intérêts propres, le processus final tendrait vers l'intérêt commun. Néanmoins, et dans les faits, cette « main invisible » n'est pas forcément fonctionnelle. Autre élément important également mis en avant par R. Binns, ces plateformes doivent impérativement être neutres, transparentes et obtenir un niveau de confiance élevé par les individus[149].

Une autre piste de réflexion à étudier serait également celle de la question de l'opacité. Ces dernières années, de vives critiques ont pu être émises envers les algorithmes et les systèmes autour du concept de « Big Data ». De la captation à la gestion en passant par la valorisation des données, les individus ne sont pas pleinement informés des pratiques. Mais, une totale transparence des systèmes est-elle la solution ? Pour Frank Pasquale, « *Transparency is not just an end in itself, but an interim step on the road to intelligibility* »[150]. En effet, le besoin de tendre vers une transparence totale n'est pas une finalité. Il faut également tendre vers une simplification des informations. Prenons l'exemple des politiques de confidentialité. A l'heure actuelle, plusieurs études montrent que les individus ne prennent pas le temps de lire ces documents denses et fastidieux pour la grande majorité d'entre eux. Une récente initiative du Conseil des consommateurs norvégien a pu mettre en lumière la complexité de ce type de publications. Le 24 mai 2016, un panel d'individus a été filmé en direct en train de lire les termes d'utilisation de trente applications différentes, de Facebook à Whatsapp en passant par Gmail et Snapchat. A cette occasion, le directeur du service digital du Norwegian Consumer Council Finn Myrstad déclarait que « la forme actuelle des

[149] BINNS, Reuben, "Personal Data Empowerment and the Ideal Observer", Faculty of Business and Law/Department of Electronics and Computer Science, University of Southampton
[150] PASQUALE, Frank, The Black Box Society, The Secret Algorithms That Controls Money and Information, Harvard University Press, 2015

conditions générales d'utilisation est à la limite de l'absurde. Leur champ d'application, leur longueur et leur complexité signifie qu'il est pratiquement impossible de prendre de bonnes décisions »[151].

Ainsi, plus qu'une transparence, il est nécessaire d'envisager une meilleure formation et information des individus sur les questions des données personnelles et de vie privée en ligne. Cette étape conduirait alors à une meilleure compréhension des pratiques actuelles et inciterait davantage à des actions par les individus afin de protéger, par eux-mêmes, leur vie privée. *In fine*, les fournisseurs de service s'orienteraient vers des modèles d'affaires plus respectueux de la vie privée de leurs utilisateurs. Cette formation des individus aux enjeux des données personnelles devrait également conduire à une réflexion plus poussée autour des outils et des utilisations des données personnelles par les individus eux-mêmes. Nous évoquions des alternatives possibles avec les plateformes de « Personal Data Management » mais d'autres voies sont également à envisager.

Ce mémoire ouvre la voie à une réflexion plus en avant sur le mouvement Quantified Self et ses implications concernant l'utilisation des données personnelles et de la vie privée de ses utilisateurs. Il est donc nécessaire de poursuivre la réflexion tant sur les questions soulevées au sein de ce mémoire que sur une pluralité de thématiques liées : la question de la dé-identification des données personnelles, la question du droit de propriété des données… La complexité du traitement de l'ensemble de ces questions est qu'elles couvrent une pluralité de domaines de recherche. Du droit à l'économie en passant par la sociologie et la psychologie sociale, les recherches sur les données personnelles doivent se poursuivre. L'un des enjeux fondamentaux de ces réflexions est bien une adaptation du droit national, européen et international aux nouveaux systèmes techniques, à leurs évolutions rapides et aux usages qu'ils permettent et qu'ils permettront.

[151] Citation issue de l'article disponible en ligne : CRAVO, Bruno, « En direct, des Norvégiens lisent toutes les conditions générales d'utilisation de trente applis » www.slate.fr/story/118523/norvege-lire-integralite-conditions-generales-utilisation, consulté le 12/05/16.

Table des annexes

Bibliographie

➢ Ouvrages

ANDERSON, Chris. *Free! Entrez dans l'économie du gratuit*. Editions Broché, 2009.

ARIELY, Dan. *Predictably Irrational: The Hidden Forces That Shapes Our Decisions*. 2008.

CHIGNARD, Simon et BENYAYER, Louis-David. *Datanomics, les nouveaux business models des données*. Editions FYP, 2015.

COLIN, Nicolas et VERDIER, Henri. *L'âge de la multitude. Entreprendre et gouverner après la révolution numérique*. Editions Armand Colin, 2012.

CARDON, Dominique. *A quoi rêvent les algorithmes ?*. La République des idées, 2015.

DELORT, Pierre. *Le Big Data*. Presses Universitaires de France, 2015.

DESROSIERES, Alain. *Pour une sociologie historique de la quantification*. Presse de l'école des Mines, 2008.

FOUCAULT, Michel. *L'origine de l'herméneutique de soi.* Conférences prononcées à Dartmouth College [1980], Vrin, 2013, p.53.

GICQUEL, Camille et GUYOT, Pierre. *Quantified Self, les apprentis sorciers du « moi connecté »*. Editions FYP, 2015.

GITELMAN, Lisa (sous la dir.). *Raw Data Is an Oxymoron*. the MIT Press, 2013.

HUSSERL, Edmond. *La crise des sciences européennes et phénoménologie transcenantes*. 1976, p.76.

LAURENT, Maryline et BOUZEFRINE, Samia. *Digital Identity Management*. 2015.

MOROZOV, Evgeny. *Le mirage numérique. Pour une politique du Big Data*. Editions Les Prairies Ordinaires, 2015.

PASQUALE, Frank. *The Black Box Society, The Secret Algorithms That Controls Money and Information.* Harvard University Press, 2015.

ROCHELANDET, Fabrice. *Economie des données personnelles et de la vie privée*. Editions La Découverte, 2010.

SADIN, Eric. *La vie algorithmique, critique de la raison numérique*. Editions L'échappée, 2015.

SCHLEE, Christian. *Targeted Advertising Technologies in the ICT Space : a Use Case Driven Analysis*. Springer Science & Business Media, 2013.

SIMON, Herbert A. *Models of Man: Social and Rational – Mathematical Essays on Rational Human Behavior in a Social Setting*. Wiley, 1957.

SIMON, Herbert A. *Theories of Bounded Rationaly*. 1972.

STUART MILL, John. *Principles of Political Economy*. 1848.

THALER, Richard H. et SUNSTEIN, Cass. R. *Nudge, la méthode douce pour inspirer la bonne décision*. Broché, 2010.

➢ Articles de recherche

ACQUISTI, Alessandro, CURTIS, Taylor et WAGMAN, Liad. The Economics of Privacy. Disponible sur <http://ssrn.com/abstract=2580411>. [Consulté le 25 février 2016]

ACQUISTI, Alessandro, MBO'O IDA Michèle Francine, ROCHELANDET Fabrice. Les Comportements de vie privée face au commerce électronique. Une économie de la gratification immédiate. *Réseaux*, 2011, n°167, pp. 105-130.

ALMUIMEDI, Hazim, SCHAUB, Florian, SADEH, Norman, ADJERID, Idris, ACQUISTI, Alessandro, GLUCK, Joshua, FAITH CRANOR, Lorrie et AGARWAL, Yuvraj. Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI'15)*, 2015.

BICZOK, Gergely et HUI CHIA, Pern. Interdependent Privacy: Let Me Share Your Data. *Financial Cryptography and Data Security*, Volume 7859 of the series Lecture Notes in Computer Science, pp 338-353.

BINNS, Reuben. Personal Data Empowerment and the Ideal Observer. Faculty of Business and Law/Department of Electronics and Computer Science, University of Southampton, 2014.

BUSH, Vannevar, "As We May Think", *Atlantic Monthly*, 1945.

CALO, Ryan. Digital Market Manipulation. *University of Washington School of Law Research Paper*, no. 2013-27, 2013.

CAMERER, Colin F. et LOEWENSTEIN, George. Behavorial Economics: Past, Present, Future. *Advances in Behavorial Economics*, Princeton University Press, 2004.

CECERE, Grazia et LE GUEL, Fabrice. Les modèles d'affaires sont-ils trop indiscrets ? *Réseaux*, n°189, 2015, pp 77-101.

CHOE, Eun Kyoung, JUNG, Jaeyeon, LEE, Bongshin et FISHER, Kristie. Nudging People Away From Privacy-Invasive Mobile Apps Through Visual Framing. *Human-Computer Interaction*, Volume 8119 of the series Lectures Notes in Computer Sciences, 2013, pp 74-91.

DETRAIGNE, Yves et ESCOFFIER, Anne-Marie. Rapport d'information fait au nom de la commission des lois, « La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information », n°441, 2009.

DIENLIN, Tobias et TREPTE, Sabine. Is the privacy paradox a relic of the past ? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, 45, 2015, pp. 285-297.

DINEV, Tamara, XU, Heng, SMITH, H. Jeff et HART, Paul. Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-related Concept. *European Journal of Information Systems*, 2013.

EGELMAN, Serge et PEER, Eyal. Predicting Privacy and Security Attitudes. *ACM SIGCAS Computers and Society*, 2015, Volume 45, Issue 1, pp 22-28.

FRIEDMAN, David Adam. Free Offers: A New Look. *New Mexico Law Review*, 2008, Vol. 38.

GRANJON, Fabien, NIKOLSKI, Véra et PHARABOD, Anne-Sylvie. Métriques de soi et Self-tracking. Une nouvelle culture de soi à l'ère numérique et de la modernité réflexive ? *Recherches en communication*, 2011, n°35.

GRAZIA, Cecere, LE GUEL, Fabrice et ROCHELANDET, Fabrice. Les modèles d'affaires numériques sont-ils trop indiscrets ? Une analyse empirique. *Réseaux*, 2015, n°186, p.77-101.

HEATH, Joseph et ANDERSON, Joel. Procrastination and the extended will. in C. Andreou & M. D. White, *The Thief of time*, Oxford University Press, 2010.

HILDEBRANDT, Mireille, O'HARA, Kieron et WAIDNER, Michael. Introduction to The Value of Personal data. 2013, *Digital Enlightenment Forum Yearbook 2013*.

IGO, Sarah E. The Beginnings of the End of Privacy. The Hedgehog Review, 2015, Vol. 17, No. 1.

JUNGLAS, Iris A., JOHNSON, Norman A. et SPITZMÜLLER, Christiane. Personality traits and concern for privacy : an empirical study in the context of location-based services. *European Journal of Information Systems*, 2008.

KELLEY, Gage Patrick, CRANOR, Lorrie Faith et SADEH, Norman. Privacy as part of App decision-making process. 2013.

KOOPS, Bert-Jaap, NEWELL Bryce Clayton, TIMAN, Tjerk, SKORVANEK, Ivan, CHOKREVSKI, Tom et GALIC, Masa. A Typology of Privacy. *University of Pennsylvania Journal of International Law*, 2016.

KORZAAN, Melinda L et BOSWELL, Katherine T. The Influence of Personality Traits and Information Privacy Concerns on Behavorial Intentions. *Journal of Computer Information Systems*, 2008.

LAFRANCE, Jean-Paul. L'économie numérique : la réalité derrière le miracle des NTIC. *Revue française de l'information et de la communication*, 2013.

LANEY, Doug. 3D Data Management: Controlling Data Volume, Velocity and Variety. 2001.

LANZING, Marjolein. The Self Transparent. *Ethics and Information Technology*, 2016, Volume 18, Issue 1, pp 9-16.

MANDEL, Michael. Beyond Goods and Services: The (Unmeasured) Rise of the Data-Driven Economy. *Policy Memo*, Progressive Policy Institute, 2012.

MILLE, Alain. Des traces à l'ère du Web. *Intellectica*, 2013, n°59, pp 7-28.

O'DONOGHUE, TED et RABIN, Matthew. The economics of immediate gratification. *Journal of Behavioral Decision Making*, 2000, Volume 13, Issue 2, pp. 233-250.

OROBON, Frédéric. Le paternalisme libéral, oxymore ou avenir de l'Etat-Providence. *Esprit*, 2013.

POSNER, Richard A. The Right of Privacy. University of Chicago Law School, 1977.

RALLET, Alain, ROCHELANDET, Fabrice et ZOLYNSKI, Célia. De la Privacy by Design à la Privacy by Using. *Réseaux*, 2015, n°189.

SHAMPAN'ER, Kristina et ARIELY, Dan,. How Small is Zero price? The True Value of Free Products. Working Papers, Federal Reserve Bank of Boston, n°06-16.

SOLOVE, Daniel J. "A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 2006, Vol. 154, n° 3, p. 477.

SMITH, H. Jeff, DINEV, Tamara et XU, Heng. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 2011.

SWAN, Melanie. The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery, 2013.

TSELIOS, S., PERKUHN, H., VANDIKAS, K. et KAMPMANN, M. Targeted Mobile Advertisement in the IP Multimedia Subsystem. in XIAN-SHENG, Hua, *Online Multimedia Advertising : Techniques and Technologies*, 2010, IGI Global.

WATHIEU, Luc et FRIEDMAN, Allan. An Empirical Approach to Understanding Privacy Valuation. Working Knowledge, Harvard Business School, 2007.

➢ Ressources en ligne

BARNES, Susan B. Privacy Paradox: Social Networking in the United States. [en ligne]. Disponible sur <https://firstmonday.org>. [Consulté le 15 janvier 2016]

BUS, Jacques and NGUYEN, M.-H. Carolyn. Personal Data Management – A Structured Discussion [en ligne]. Disponible sur <https://digitalenlightment.org>. [Consulté le 20 avril 2016]

BUTLER, Sarah et GLASGOW, Garrett. The Value of Personal Information to Consumers of Online Services: Evidence from a Discrete Choice Experiment". [en ligne]. Disponible sur <http://www.nera.com>. [Consulté le 20 juin 2016]

CALABRESE, Chris, MCINNIS, Katherine L., HANS, G.S. et NORCIE, Greg. Comments for November 2015 Workshop on Cross-Device Tracking. [en ligne]. Disponible sur <https://cdt.org/>. [Consulté le 8 mars 2016]

CIGREF. L'économie des données personnelles : les enjeux d'un business éthique. [en ligne]. Disponible sur <http://cigref.fr/>. [Consulté le 25 janvier 2016]

CISCO. Networking Index: Global Mobile Data Traffic Forecast Update, 2015-2020. [en ligne]. Disponible sur <https://www.cisco.com>. [Consulté le 12 mars 2016]

COLLIN, Pierre et COLIN, Nicolas. Mission d'expertise sur la fiscalité du numérique de 2013. [en ligne]. Disponible sur <http://www.economie.gouv.fr/> [Consulté le 30 avril 2016]

CORBIN, Kenneth. What happens with data from mobile health apps? [en ligne]. Disponible sur <http://cio.com/> [Consulté le 17 avril 2016]

CROVITZ, L. Gordon. Avira Will Regulators Unfriend Facebook? *The Wall Street Journal*. [en ligne]. Disponible sur <http://wsj.com> [Consulté le 7 mars 2016]

FRINK, Lyle. Avira now identifies SilverPush ad-tracking as malware. [en ligne]. Disponible sur <http://blog.avira.com/>. [Consulté le 7 mars 2016]

HILDEBRANDT, Mireille. Slaves to Big Data. Or Are we? [en ligne]. Disponible sur <http://works.bepress.com> [Consulté le 12 mai 2016]

KING, Jennifer. Understanding Privacy Decision-Making Using Social Exchange Theory. [en ligne]. Disponible sur <http://networkedprivacy2015.files.wordpress.com> [Consulté le 21 avril 2016]

LACROIX, Dominique. Slaves Le blues du Net, par Bernard Stiegler. [en ligne]. Disponible sur <http://reseaux.blog.lemonde.fr> [Consulté le 7 mai 2016]

LIU, Bin, ANDERSEN, Mads Schaarup, SCHAUB, Florian, ALMUHIMEDI, Hazim, SADZH, Norman, AGARWAL, Yuvraj et ACQUISTI, Alessandro. To Deny or Not to Deny: A Personalized Privacy Assistant for Mobile Apps Permission. [en ligne]. Disponible sur <https://www.ftc.org>. [Consulté le 20 mai 2016]

MACCARTHY, Mark. New Directions in Privacy: Disclosures, Unfariness and Externalities. [en ligne]. Disponible sur <http://www18.georgetown.edu/> [Consulté le 25 avril 2016]

MCFARLAND, Michael. Unauthorized Transmission and use of Personal Data. [en ligne]. Disponible sur <http://www.scu.edu/> [Consulté le 5 mai 2016]

MOTTL, Judy. FTC: Health, fitness apps share user info with vendors. *Fierce Mobile Healthcare*. [en ligne]. Disponible sur <http://www.fiercemobilehealthcare.com [Consulté le 27 avril 2016]

MYRSTAD, Finn. Complaint concerning the mobile phone app Runkeeper. [en ligne]. Disponible sur <http://fbrno.climg.no/>. [Consulté le 1er juin 2016]

OECD, Exploring the Economics of Personal Data : A Survey of Methodologies for Measuring Monetary Value. *OECD Digital Economy Papers* [en ligne]. 2013, n°220, OECD Publishing, Paris.

President's Council of Advisors on Science and Technology. Report to the President: Big Data and Privacy: A Technological Perspective 2014. [en ligne]. Disponible sur https://www.whitehouse.gov/. [Consulté le 26 mai 2016]

PULTIER, Antoine, HARRAND, Nicolas et BAE BRANDTZAEG, Petter. Report: Privacy in Mobile Apps. [en ligne]. Disponible sur <http://fbrno.climg.no/>. [Consulté le 1er juin 2016]

SPIKERMANN, Sarah, KORUNOVSKA, Jana et BAUER, Christine. Psychology of Ownership and Asset Defense: Why People Value Their Personal Information Beyond Privacy. [en ligne]. Disponible sur <htts://epub.wu.ac.at> [Consulté le 15 juin 2016]

STEEL, Emily et DEMBOSKY, April. Health apps run into privacy rugs. *The Financial Times*. [en ligne]. Disponible sur <http://www.ft.com> [Consulté le 14 avril 2016]

SWAN, Melanie. The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery. [en ligne] Disponible sur <https://www.cs.swarthmore.edu/>. [Consulté le 3 avril 2016]

THOMSON, Iain. How TV ads silently ping commands to phones: Sneaky SilverPush code reverse-Engineered [en ligne]. Disponible sur <http://www.theregister.co.uk/>. [Consulté le 9 mars 2016]

World Economic Forum. Rethinking Personal Data : Strenghtening Trust. [en ligne]. Disponible sur <https://www3.weforum.org>. [Consulté le 2 février 2016]

ZANG, Jinyan, DUMMIT, Krysta, GRAVES, James, LISKER, Paul et SWEENEY, Latanya. Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps. [en ligne] Disponbible sur <jots.pub >. [Consulté le 12 janvier 2016]

Table des matières