Etude de marché sur la perception des consommateurs relative aux données collectées par les sites internet et applications web. Application aux cas de Google et Facebook.

Auteur : Carretta, Yves
Promoteur(s) : Ghilissen, Michael
Faculté : HEC-Ecole de gestion de l'Université de Liège
Diplôme : Master en sciences de gestion, à finalité spécialisée en management général (Horaire décalé)
Année académique : 2017-2018
URI/URL : http://hdl.handle.net/2268.2/5284

Etude de marché sur la perception des consommateurs relative aux données collectées par les sites internet et applications web. Application aux cas de Google et Facebook.

Promoteur :
Prof. Michael Ghilissen
Lecteur:
Prof. Marc Alexandre

Travail de fin d'études présenté par
Yves CARRETTA
En vue de l'obtention du diplôme
de Master en sciences de gestion,
à finalité spécialisée en management général
Année académique 2017/2018

Résumé :

Au cours de la dernière décennie, nous avons assisté à de profonds changements dans grâce à la part grandissante qu'occupe internet dans nos vies. Notre manière d'interagir avec nos amis, de consommer, de nous informer a beaucoup évolué. Nous avons désormais accès à une énorme quantité d'informations grâce à nos smartphones qui nous permettent de rester connectés à tout moment. En utilisant nos smartphones ou en surfant sur internet, les sites et plateformes auxquelles nous accédons collectent des informations à notre sujet pour améliorer notre expérience de navigation mais aussi pour nous proposer entre autre de la publicité ciblée. Dans ce contexte, l'objectif de ce travail est de faire un état des lieux, de comprendre la position des consommateurs par rapport aux données collectées à leur sujet. En sont-ils conscients ? Y sont-ils favorables ? Y voient-ils un danger ? Comment réagissent-ils par rapport aux récents scandales liés aux données Facebook et aux objets connectés ? Pour ce faire, nous avons effectué une étude de marché qualitative auprès de 8 personnes. Ce travail présente la méthodologie utilisée et les principaux résultats obtenus.

Remerciements

Avec ce travail, je mets un point final à deux années de cours du soir très enrichissantes. J'ai pu rencontrer des personnes très intéressantes, me faire de nouveaux amis, découvrir de nouveaux points de vue et obtenir une vue globale du fonctionnement d'une entreprise. Cette formation m'a demandé beaucoup d'investissement personnel, mais cela en valait la peine.

Je souhaite remercier toutes les personnes qui ont contribué, de près ou de loin, à la rédaction de ce travail de fin d'études. En particulier :

- Monsieur Ghilissen pour ses conseils et pour avoir accepté d'être mon promoteur ;
- Monsieur Alexandre pour avoir accepté de faire partie du jury ;
- Un grand merci à tous ceux qui ont pris le temps de répondre à mes questions dans le cadre de mon enquête ;

Enfin, je remercie mes parents, mon entourage et mes amis pour leur soutien dans le cadre de ce master en cours du soir.

Table des matières

Introduction

Au cours de la dernière décennie, les géants de l'internet que sont Google, Apple, Facebook et Amazon ont profondément changé nos vies. Ces entreprises ont eu un impact sur la manière dont nous interagissons avec nos amis, nos connaissances, voire des personnes qui nous sont étrangères grâce à Twitter par exemple. L'internet a fait tomber certaines barrières ce qui permet de mettre les entreprises, les marques au plus près de leur clientèle existante mais aussi de clients potentiels.

La manière dont nous consommons grâce au commerce en ligne a également été impactée. Il est désormais très facile de faire des achats sur internet, que ce soit des vêtements via la plateforme Zalando, ses courses alimentaires où les enseignes de grande distribution présentes en Belgique proposent ce type de services : «Carrefour drive», «Delhaize.be» et «Collect&Go» de Colruyt ou encore en utilisant Amazon pour trouver une gamme de produits plus générale (livres, articles électroniques, vêtements, etc.)

Des services « gratuits » tels que ceux offerts par Google nous permettent de communiquer (Gmail, Hangout), d'effectuer efficacement des recherches sur Internet via le moteur de recherche Google et l'application Google-Chrome ou encore de trouver le meilleur itinéraire chaque jour et en temps réel grâce à Waze, une application de trafic et de navigation communautaire.

L'accès à l'information passe davantage par internet ; tous les grands quotidiens ont désormais une plateforme en ligne accessible aux abonnés ou non-abonnés. De plus en plus de personnes s'informent également via des « posts » Facebook publiés par ces médias dits « traditionnels » (quotidiens, magazines hebdomadaires, chaines de télévision ou de radio, etc.)

La popularisation du smartphone par des marques telles que Apple et Samsung nous permet de rester connecté en permanence, d'avoir accès aux différents services mentionnés ci-dessus à tout moment et de partager avec nos connaissances des informations sur les activités que nous sommes en train de faire, les lieux que nous fréquentons, nos destinations de vacances, notre opinion sur le dernier restaurant visité, etc.

Ce faisant nous dévoilons énormément d'informations à notre sujet. Ces informations peuvent ensuite être utilisées à des fins de marketing pour proposer de la publicité plus ciblée qu'avec les canaux traditionnels ou pour suggérer de nouveaux produits sur base des informations collectées lors des achats précédents. Ceci est évidemment à l'avantage des entreprises qui investissent dans la collecte de données et dans des outils d'analyse. En effet, comme chacun le sait, une bonne connaissance des attentes du marché est capitale pour le développement des nouveaux produits. Le client perçoit également des aspects positifs, celui-ci se voit proposer des produits qui correspondent à ses attentes ainsi que des services en ligne gratuits (Gmail, Google Maps, Facebook, etc.), ceci occasionne des gains de temps, permet de découvrir des articles, des évènements, des endroits à visiter, …

Le cas évoqué ci-dessus fait écho à une situation « win-win » où entreprises et clients bénéficient tous deux de ces échanges. On l'a vu dernièrement avec le scandale « Cambridge Analytica » les informations personnelles des internautes peuvent être utilisées à des fins politiques pour tenter d'influencer l'opinion avant une élection, dans le cas de cette affaire, des soupçons de manipulation

des électeurs pèsent sur les dernières élections présidentielles aux Etats-Unis ainsi que sur le référendum du Brexit.

Les données collectées par les applications que l'on utilise au quotidien permettent d'en connaitre énormément à notre sujet. Ainsi dans le documentaire « Nothing to hide », un acteur Luxembourgeois vivant à Berlin, accepte de placer un mouchard sur son smartphone et son ordinateur portable collectant des données telles que la position GPS, les heures d'utilisation de son smartphone, le type de recherches effectuées sur google, le nombre de messages reçus, etc.

Ces données similaires à celles collectées par Facebook, Google, etc. ont permis de déterminer ses heures de lever et de coucher, son niveau de richesse, son cercle d'amis, d'avoir un aperçu de ses opinions politiques, etc.

L'utilisation de ces données par des organismes d'assurance par exemple pourrait avoir un impact sur le montant des primes à payer ou à l'extrême sur le fait de pouvoir bénéficier ou non d'une assurance.

L'objectif de ce travail est de faire un état des lieux, de comprendre la position des consommateurs par rapport aux données collectées à leur sujet. En sont-ils conscients ? y sont-ils favorables ? y voient-ils un danger ? Comment réagissent-ils par rapport aux récents scandales liés aux données Facebook et aux objets connectés ?

Quelle valeur associent-ils aux données qu'ils partagent au quotidien ? Quelle contrepartie attendent-ils ? Estiment-ils que leurs données ont une valeur ? Sont-ils prêts à partager davantage d'informations pour obtenir des réductions, des offres personnalisées ? Mais aussi quelle est la limite, quel seuil ne souhaitent-ils pas franchir.

Pour répondre à ces questions, nous avons effectué une étude de marché qualitative. Nous estimons que celle-ci se prête bien au sujet qui nous occupe : une quinzaine de questions ouvertes a été posée individuellement à 8 personnes d'âges et d'horizons différents. Afin de réduire la portée des questions, nous avons décidé de les axer sur les questions sur l'utilisation de Google et de Facebook. En effet, ces deux outils sont très largement utilisés et font pour ainsi dire partie de nos vies.

Le premier chapitre de ce travail fait un tour d'horizon des avantages de l'utilisation des données collectées par ces entreprises via des outils « Big Data » qui permettent de déterminer les tendances, faire des prédictions, segmenter le marché de manière très fine etc.

Le second chapitre, illustre par différents exemples, les inconvénients, risques et dangers liés à une mauvaise utilisation de ces données; pour les particuliers qui risquent de voir leur vie privée exposée au grand jour mais aussi pour les entreprises qui pourraient ainsi se retrouver dans la tourmente et par là même pourraient perdre la confiance de leurs clients.

Le troisième chapitre aborde les règles principales relatives à la protection des données en vigueur en Belgique mais aussi au niveau Européen avec le nouveau règlement sur la protection des données (GPDR) entré en vigueur fin mai 2018. Le quatrième chapitre présente les questions posées ainsi qu'une analyse des réponses apportées par les personnes interrogées.

Chapitre 1 – Opportunités liées à l'utilisation des technologies big data pour les entreprises/particuliers

1.1.Introduction

La quantité de données générées à l'échelle mondiale a augmenté de manière exponentielle au cours de ces dernières années (cf. Figure 1). Cette tendance résulte d'une utilisation croissante des réseaux sociaux (cf. Figure 2) ; un réseau social comme Facebook compte actuellement 2.1 milliards d'utilisateurs [1]. Via ces plateformes, nous pouvons rester en contact avec nos connaissances, nos amis,… Nous pouvons partager nos centres d'intérêts, nous inscrire à des évènements, etc. Ces services sont désormais accessibles à tout moment, via notre ordinateur ; dans le cadre privé mais aussi au bureau, ou via tablette ou smartphone. D'après une étude effectuée en 2017 par le bureau d'études de marchés Ivox, 78.5% des Belges possèdent un smartphone qu'ils portent en moyenne 9h par jour [2].

L'utilisation des objets connectés tels que les smartphones génère elle aussi un grand nombre de données. En effet, grâce à eux nous avons facilement accès à nos e-mails, nous pouvons effectuer des achats en ligne, retrouver notre chemin grâce au GPS intégré, consulter les sites d'informations en ligne, etc.

Notre utilisation des smartphones et des réseaux sociaux génère énormément d'informations à notre sujet ; habitudes de vie, centres d'intérêts, achats effectués, lieux visités, groupes d'amis etc.

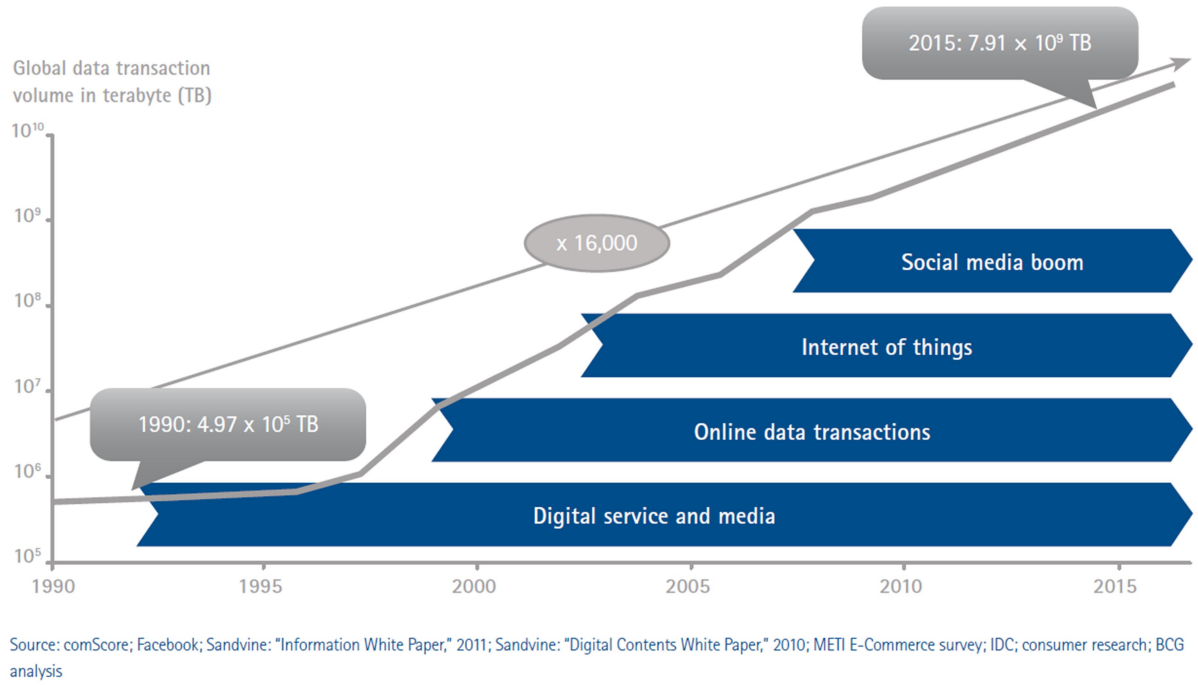

Figure 1. Evolution de la quantité de données échangées à l'échelle mondiale au cours du temps [3]. On assiste à une augmentation exponentielle des données générées en raison de l'utilisation des objets connectés et des réseaux sociaux.

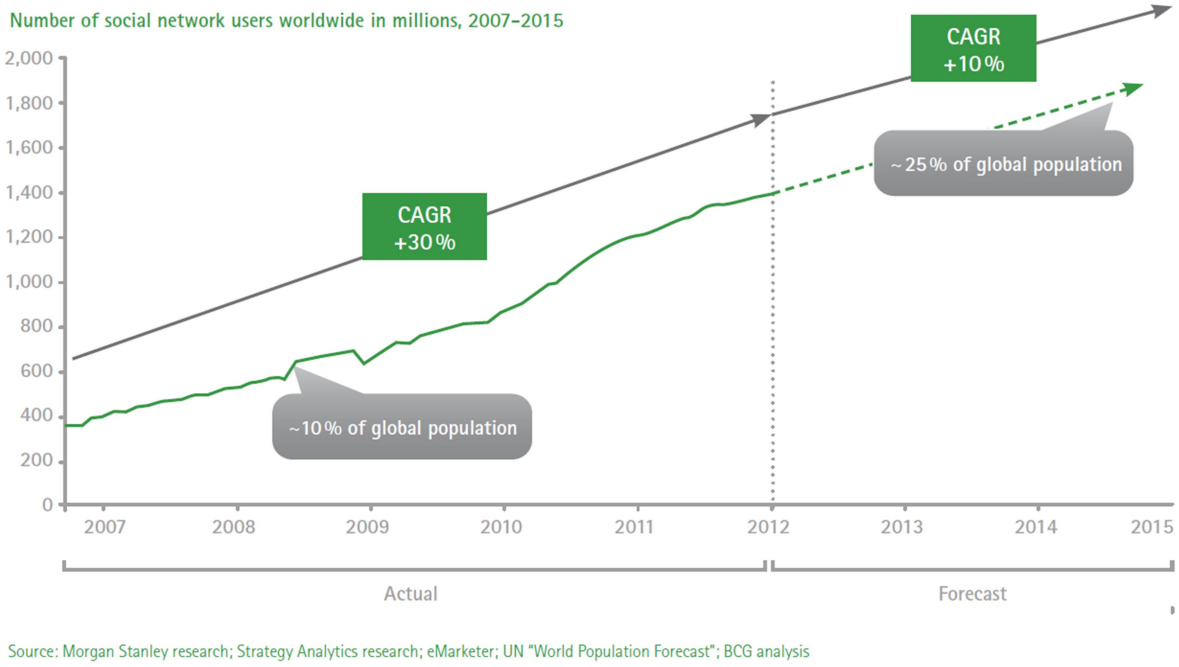

Figure 2. Evolution du nombre d'utilisateurs des réseaux sociaux à l'échelle mondiale [3].

Dans le même temps, les infrastructures et les techniques permettant de traiter de grandes quantités de données se sont développées (cf. Figure 3) : ce traitement d'une grande quantité d'informations - qui hier encore était réservé à des sociétés très spécialisées - est aujourd'hui devenu plus accessible, on parle de « Big Data ». Ce terme comprend un grand nombre de définitions [4], on se réfèrera ici à la définition suivante : le big data est le « *domaine technologique dédié à l'analyse de très grands volumes de données informatiques (petaoctets), issus d'une grande variété de sources, tels les moteurs de recherche et les réseaux sociaux* » [5].

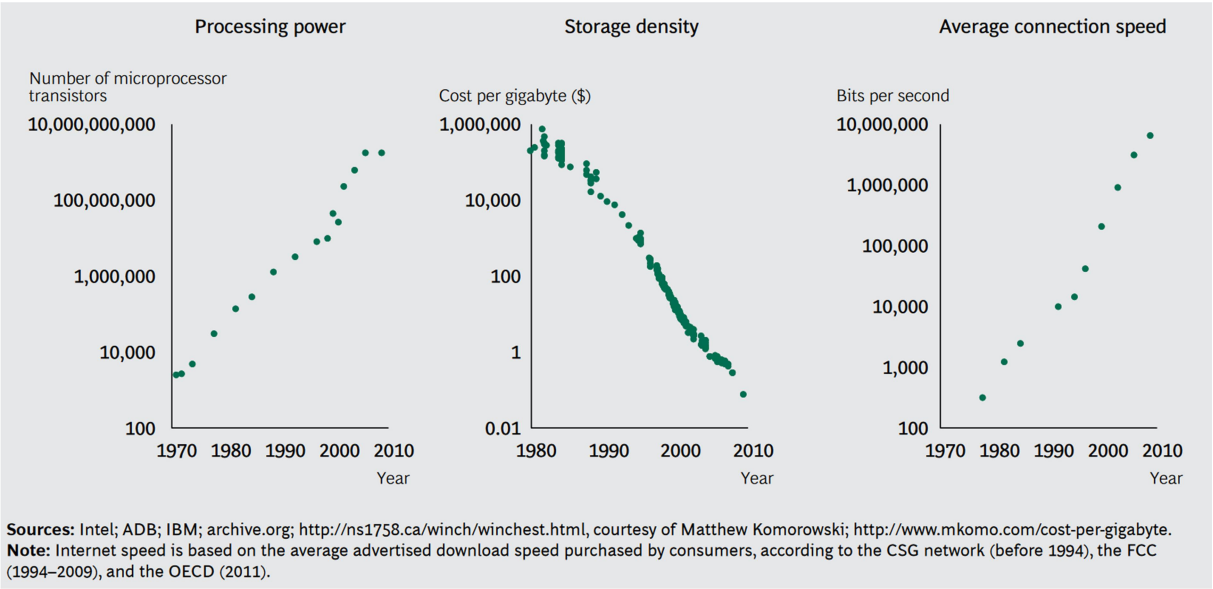

Figure 3 Evolution de la vitesse des processeurs, du coût de la mémoire utilisés dans les systèmes électroniques et de la vitesse de connexion au cours du temps : ces différentes tendances vont toutes dans le sens d'une plus grande rapidité du traitement des données et d'une diminution du coût le rendant plus accessible [6].

1.2.Gains potentiels et « success story »

Le traitement de ces données représente un gisement de valeurs inépuisable pour qui sait les utiliser. Un document de Bain&Company [7] estime qu'en 2015, de gros investissements ont été consentis à l'échelle mondiale dans différents secteurs :

- services financiers : 6.4 Milliards de dollars
- internet/logiciels : 2.8 Milliards de dollars
- gouvernement : 2.8 Milliards de dollars
- communication médias : 1.2 Milliards de dollars
- énergie : 800 Millions de dollars

Cette même référence indique que les sociétés qui utilisent les technologies du « *Big Data* » ont

- 5 fois plus de chances de prendre des décisions plus rapidement que leurs concurrents
- 3 fois plus de chances d'exécuter les décisions prises initialement
- 2 fois plus de chances d'avoir un rendement financier se situant dans le quartile supérieur
- 3 fois plus de chances d'obtenir une croissance annuelle supérieure à 10% [8]

The Boston Consulting Group [3] estime que les bénéfices engendrés par l'utilisation des données personnelles peuvent atteindre globalement 1 000 milliards d'Euros d'ici 2020. Les données personnelles sont en quelque sorte une nouvelle forme de monnaie [9].

La référence [3] cite différentes manières utilisées par les organisations pour tirer profit de l'utilisation des données personnelles. Les différents niveaux sont décrits ci-dessous et représentés sur la Figure 4.

- **Automatisation du procédé d'identification:** en intégrant les données personnelles dans leurs procédures, les entreprises peuvent simplifier et accélérer les étapes d'identifications en gardant en mémoire les préférences de chacun des utilisateurs. Ce faisant, l'expérience de l'utilisateur est améliorée puisque celui-ci se voit proposer un service correspondant directement à ses attentes. Par exemple, un utilisateur régulier d'une compagnie aérienne pourra effectuer une réservation sans devoir encoder son numéro de passeport, la position du siège (allée, hublot, etc.), etc.
- **Personnalisation des produits et des services:** dans ce cas, les consommateurs se voient proposer une offre personnalisée sur base de leurs achats précédents, de leur historique de recherches, ou même via leur position GPS. Amazon propose ce type d'offre ce qui représente 25% de ses ventes.
- **Utilisation des données collectées pour guider les opérations de Recherches et Développements:** en utilisant les informations provenant des réseaux sociaux, les avis des consommateurs voire même les données provenant des capteurs des objets actuels, les entreprises peuvent obtenir des indications permettant de définir au mieux la direction à suivre pour les développements futurs. Ainsi des entreprises comme Caterpillar, Rolls Royce Aerospace et Tesla utilisent des données collectées sur les machines en service pour améliorer leurs produits [10]
- **Monétisation des données auprès de tiers:** la vente de données collectées est également une source de revenus. Prenons par exemple le cas de la chaine de supermarchés Tesco,

celle-ci a mis en place Dunnhumby, une filiale qui vend et analyse les données des habitudes d'achats des clients possédant une carte de fidélité « Club Card ». Ces données anonymisées (ne permettant pas d'identifier le consommateur) sont proposées à des sociétés comme Unilever, Nestlé ou Heinz. Cette filiale a généré en 2012 un revenu de 53 millions de Livre Sterling [11].

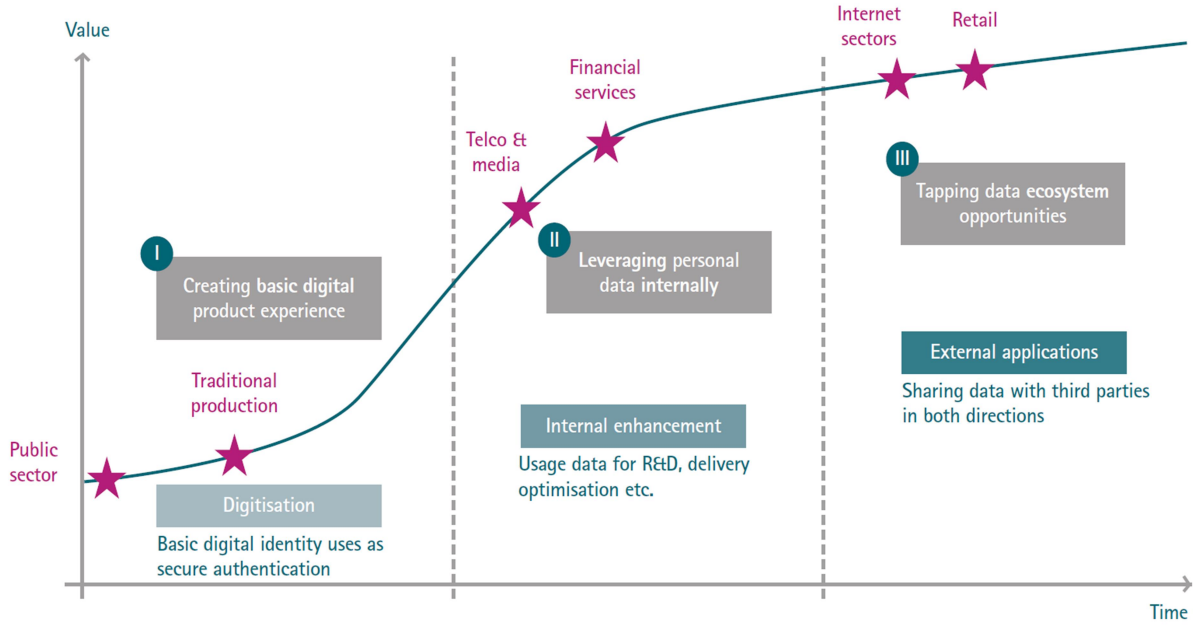

Figure 4. Evolution de la création de valeur grâce aux données personnelles [3].

Les trois grandes méthodes identifiées par [11] pour tirer profit de la vente des données collectées sont représentées sur la Figure 5. La première méthode réunit plusieurs entreprises dans une relation de partenariat pour proposer à leurs clients un meilleur service. C'est par exemple le cas de National Australia Bank qui partage les données issues des transactions électroniques de ses clients (données anonymisées ne permettant pas d'identifier les clients individuellement) avec la société d'analyse de données Quantium qui revend ensuite les résultats de ses analyses à des tiers.

Les entreprises qui achètent ces données peuvent alors compléter les données dont elles disposent déjà en interne pour créer de nouveaux produits, de nouveaux services, etc. C'est la situation centrale « *Contractual* » représentée au centre de la Figure 5. Le dernier cas de figure représenté sur cette figure a déjà été évoqué plus haut avec l'exemple de la chaine de supermarchés Tesco.

Cette vente de données peut se faire avec différents niveaux de personnalisation allant du commerce de masse pour des données générales à des approches plus personnalisées et donc plus coûteuses. Le paiement peut lui aussi se faire sous différentes formes allant du paiement à l'usage à l'abonnement. Les différentes combinaisons sont illustrées sur la Figure 6.

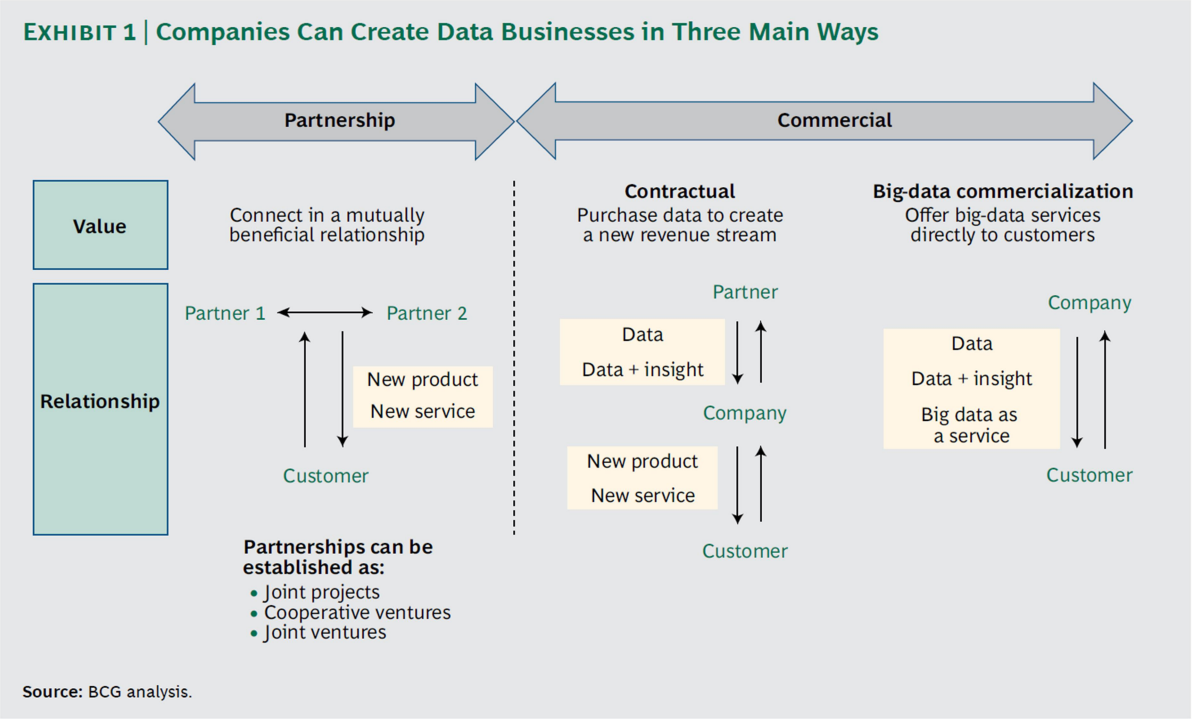

Figure 5. Représentation des trois méthodes identifiées par « *The Boston Consulting Group* » permettant aux entreprises désireuses de commercialiser les données dont elles disposent [11].

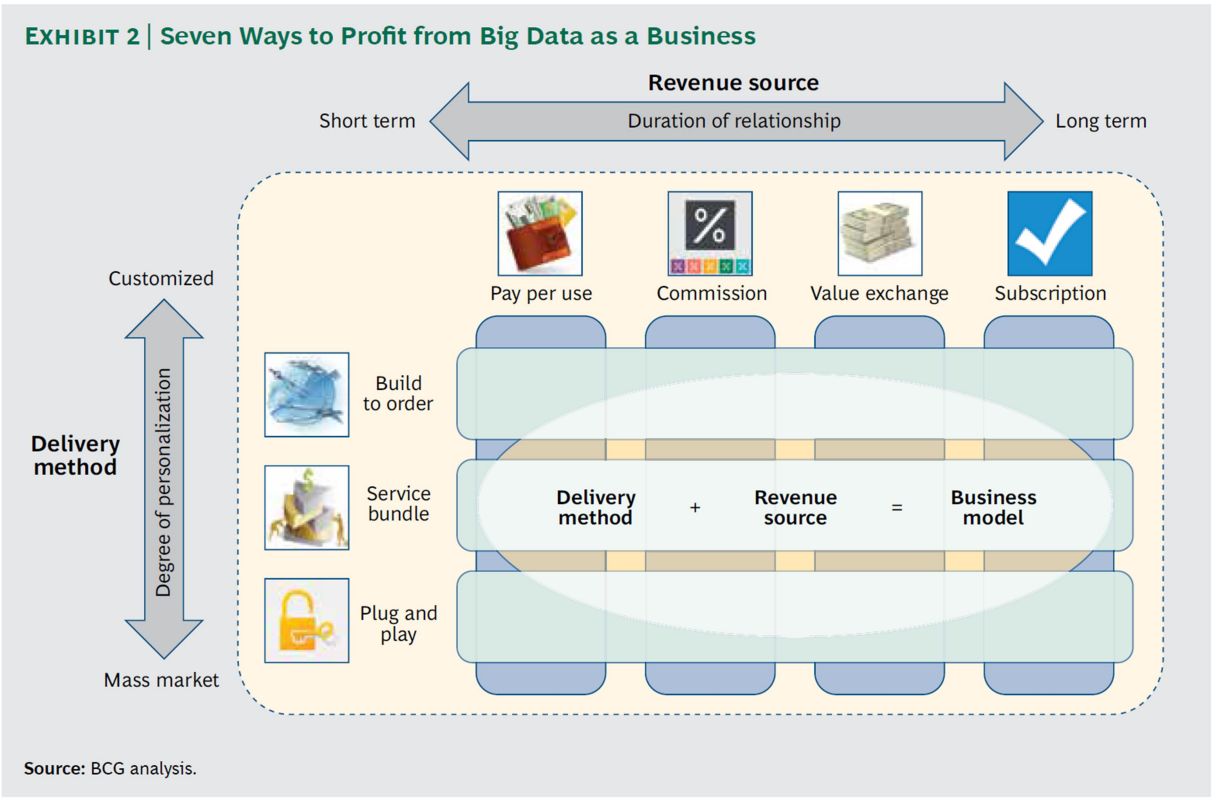

Figure 6. Commercialisation de données personnelles: représentation des différentes combinaisons possibles entre le niveau de personnalisation des analyses effectuées et le moyen de paiement [11].

Le « big data » ne bénéficie pas qu'aux entreprises privées, les institutions publiques peuvent également en tirer avantage pour réduire leurs coûts de fonctionnement ou utiliser au mieux les ressources dont elles disposent. L'Italie a par exemple mis en place un système de détection de fraude appelé « *Redditometro* » qui croise des données issues de différentes institutions telles que les crédits hypothécaires, les frais d'inscriptions scolaire des enfants, le type de voiture, l'abonnement dans des centres sportifs, etc. Les montants associés à chacun de ces éléments sont comparés avec les revenus déclarés. Ce système a permis en 2011 de récupérer un total de 11.5 milliards d'Euros [3].

Le remboursement des soins de santé pourrait également bénéficier des avancées du « big data » en effet en digitalisant l'ensemble des données médicales associées aux patients, ceux-ci pourraient être traités sur base de leur historique global et non plus uniquement sur base des symptômes actuels. De même, les traitements et dosages pourraient être adaptés patient par patient ce qui pourrait conduire à des traitements plus efficaces, une réduction des effets secondaires et une réduction des couts pour les organismes de sécurité sociale. Grâce à cette amélioration, les patients bénéficient d'une vie plus longue et donc plus productive. L'impact total à l'échelle mondiale estimé par McKinsey va de 2 à 10 trillions de dollars [12].

Les données issues de capteurs et caméras de vidéosurveillance situés en ville et en périphérie permettraient de fluidifier le trafic en redirigeant celui-ci vers les parties les moins engorgées des villes. On parle de « Smart Cities ». Ceci pourrait également avoir un impact économique important.

McKinsey [12] décrit le potentiel des méthodes de « *machine learning* » pour le traitement des données collectées. Par opposition aux algorithmes dits « traditionnels » - constitués d'instructions implémentées par un informaticien avant l'exécution du code – les algorithmes de « *machine learning* » sont obtenus sur base d'une méthode générale d'apprentissage appliqué à l'analyse d'un très grand nombre de données appelées « *training data* ». L'algorithme apprend en quelque sorte de ces expériences avant d'appliquer ces connaissances à de nouvelles situations.

Les méthodes de « *machine learning* » peuvent être appliquées à 3 grandes catégories de problèmes (cf. Figure 7) [12] :

- **problèmes de classification** qui permettent d'identifier du texte, des contenus audios et de reconnaitre des images et des vidéos. Cette méthode peut également être utilisée pour segmenter le marché
- **problèmes de prédiction** très utiles pour déterminer la probabilité associée à certains évènements ou faire des prévisions sur les ventes par exemple.
- **problème de génération** où un contenu nouveau (texte, image, etc.) est créé sur des caractéristiques similaires à des contenus existants.

Machine learning can help solve classification, prediction, and generation problems

Classification	Classify/label visual objects	Identify objects, faces in images and video
	Classify/label writing and text	Identify letters, symbols, words in writing sample
	Classify/label audio	Classify and label songs from audio samples
	Cluster, group other data	Segment objects (e.g., customers, product features) into categories, clusters
	Discover associations	Identify that people who watch certain TV shows also read certain books
Prediction	Predict probability of outcomes	Predict the probability that a customer will choose another provider
	Forecast	Trained on historical data, forecast demand for a product
	Value function estimation	Trained on thousands of games played, predict/estimate rewards from actions from future states for dynamic games
Generation	Generate visual objects	Trained on a set of artist's paintings, generate a new painting in the same style
	Generate writing and text	Trained on a historical text, fill in missing parts of a single page
	Generate audio	Generate a new potential recording in the same style/genre
	Generate other data	Trained on certain countries' weather data, fill in missing data points for countries with low data quality

SOURCE: McKinsey Global Institute analysis

Figure 7. Trois grandes catégories de problèmes répertoriés par McKinsey auxquelles les méthodes de « *machine learning* » peuvent être appliquées [12].

Dans une étude réalisée auprès de 600 entreprises, McKinsey [12] a identifié différents types de situations qui pourraient bénéficier des méthodes de « *machine learning* ». Celles-ci sont représentées sur la Figure 8. Sur cette figure, les axes verticaux et horizontaux représentent respectivement la quantité de données disponibles et l'impact du « *machine learning* » basé sur les résultats de l'enquête. Les résultats qui ont le plus de potentiel sont représentés dans la partie supérieure droite de la figure.

La référence [12] classe les applications au plus haut potentiel en 4 catégories :

- **La personnalisation** des produits et services dans les secteurs tels que biens de consommation emballés, les assurances, les médias, etc.
- **Les analyses prédictives** (« predicitve analytics ») cet ensemble englobe la segmentation du marché en fonction des historiques d'achats, du risque de désabonnement ainsi que des applications telles que la détection des fraudes bancaires
- **Optimisation** « strategic optimization » de la disposition des produits dans les rayons des supermarchés, du travail en équipe dans les entreprises, etc.
- L'optimisation des opérations de fabrication et de logistique en temps réel

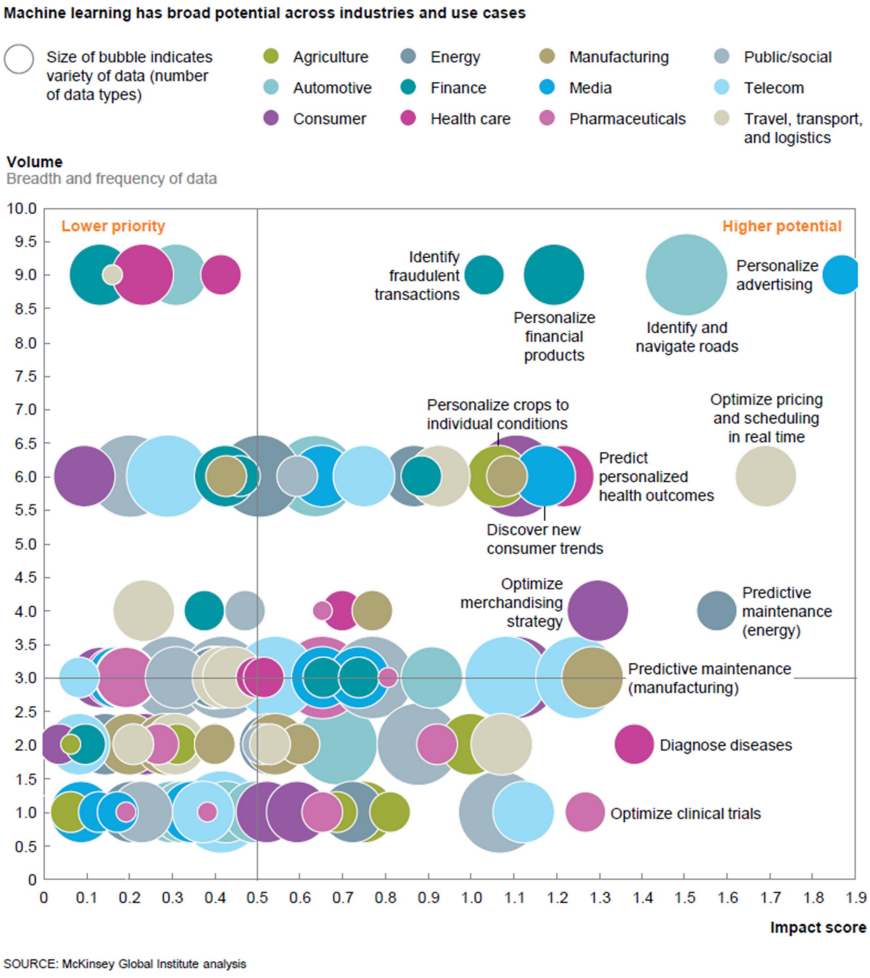

Figure 8. Potentiel des méthodes de « *machine learning* » identifiées par McKinsey [12] lors d'une étude réalisée auprès de 600 entreprises. Les applications les plus prometteuses sont répertoriées dans le coin supérieur droit de la figure.

1.3.Stratégie à mettre en place pour effectuer la transition vers l'utilisation des données collectées/changement de culture requis

En 2011 un rapport de McKinsey [13] identifiait le potentiel de l'utilisation du « *Big Data* » dans différents secteurs tels que la vente au détail aux USA, la fabrication à l'échelle mondiale, le secteur publique en Europe et le système des soins de santé aux USA. Ces chiffres ont été revisités en 2016 [12] (cf. Figure 9) et l'analyse montre que seule une fraction des gains potentiels évalués en 2011 a été atteinte et ce pour l'ensemble des secteurs cités ci-dessus.

There has been uneven progress in capturing value from data and analytics

	Potential impact: 2011 research	Value captured %	Major barriers
Location-based data	▪ $100 billion+ revenues for service providers ▪ Up to $700 billion value to end users	50–60	▪ Penetration of GPS-enabled smartphones globally
US retail[1]	▪ 60%+ increase in net margin ▪ 0.5–1.0% annual productivity growth	30–40	▪ Lack of analytical talent ▪ Siloed data within companies
Manufacturing[2]	▪ Up to 50% lower product development cost ▪ Up to 25% lower operating cost ▪ Up to 30% gross margin increase	20–30	▪ Siloed data in legacy IT systems ▪ Leadership skeptical of impact
EU public sector[3]	▪ ~€250 billion value per year ▪ ~0.5% annual productivity growth	10–20	▪ Lack of analytical talent ▪ Siloed data within different agencies
US health care	▪ $300 billion value per year ▪ ~0.7% annual productivity growth	10–20	▪ Need to demonstrate clinical utility to gain acceptance ▪ Interoperability and data sharing

1 Similar observations hold true for the EU retail sector.
2 Manufacturing levers divided by functional application.
3 Similar observations hold true for other high-income country governments.

SOURCE: Expert interviews; McKinsey Global Institute analysis

Figure 9. Impact potentiel du « big data » répertorié par McKinsey en 2011 dans différents secteurs de l'économie mondiale et pourcentage de valeur capturée en 2016 : pour chacun de secteurs listés dans le tableau, seule une partie des gains potentiels a été réalisée [12].

D'après McKinsey, cet écart entre bénéfices possibles et bénéfices réalisés vient du fait que les entreprises ont consenti des investissements importants pour acquérir de nouvelles capabilités liées au « *Big Data* », pour engager de nouveaux talents dans le domaine. Cependant, ils n'ont pas réalisé les changements d'organisation nécessaires pour en tirer le maximum.

Dans une étude réalisée auprès de dirigeants effectuant une phase de transition pour intégrer le big data dans leur entreprise, trois quart des répondants ont indiqué l'amélioration de leurs revenus où leur réduction de coûts était inférieure à 1% [14].

Cette phase de transition représente en effet un défi de taille. En effet en dehors des sociétés telles que Amazon, Google, Facebook, Netflix, Uber qui se sont construites sur un modèle digital, les entreprises ayant une histoire plus longue, font parfois face à des dirigeants seniors rétiçants à l'idée d'accroître leurs investissements dans le « *big data* » car les efforts initiaux n'ont pas amené

suffisamment de résultats. Ensuite, le personnel amené à utiliser les outils du « big data » pour améliorer les prises de décision manque parfois de confiance dans ces nouveaux outils ou ne comprennent tout simplement pas leur fonctionnement ou recommandations [15].

Jeff Immelet, le CEO de General Electric, déclare à propos des changements opérés dans son entreprise « *je pensais que c'était entièrement une question de technologie, je pensais que si nous engagions quelques milliers de personnes, que si nous mettions à jours nos logiciels, ce serait terminé. J'avais tort, les Product managers, les commerciaux, le service après-vente doivent être différents* » [14].

Un article de McKinsey [12] décrit les différentes étapes - représentées schématiquement sur la Figure 10 - qu'elle préconise pour effectuer une transition réussie :

- **Etape 1:** se poser les questions fondamentales : « *A quoi l'analyse de données sera-t-elle utilisée ? Comment les enseignements tirés de cette analyse seront-ils utilisés pour créer de la valeur ? Comment cette création de valeur sera-t-elle mesurée ? »*
- **Etape 2:** mettre en place les infrastructures techniques permettant la collecte des données
- **Etape 3:** mettre en place les outils permettant l'analyse de données collectées
- **Etape 4:** changer les procédures de décisions pour intégrer les résultats issus des données analysées
- **Etape 5:** former les personnes prenant les décisions sur base des analyses mentionnées ci-dessus afin de leur donner une vue d'ensemble des techniques utilisées, de leur fonctionnement, etc. Ceci dans le but de les aider à tirer le maximum de ces résultats mais aussi à accepter l'utilisation de ces nouveaux outils.

Le lecteur intéressé pourra également se référer à [16].

Le leadership et une bonne intégration des nouveaux outils dans l'organisation ont une importance capitale. La Figure 11 illustre les 4 types de changement d'organisation répertoriés par Bain&Company [7] pour intégrer le « big data » dans leurs processus. Le siège central peut diriger l'ensemble des opérations, identifier et définir les priorités (cas #3). Les filiales ou départements de l'entreprise peuvent également effectuer ces opérations avec ou sans l'aide du siège central (respectivement cas #1 et #3). Une autre alternative est de déléguer les choix à effectuer à un centre d'excellence qui coordonne les opérations effectuées aux différents niveaux de l'entreprise.

Une étude réalisée par McKinsey en 2016 [17], montre que pour les entreprises qui ne réussissent pas à tirer un avantage significatif des analyses de données. Cela vient d'un manque de soutien du leadership, une mauvaise communication et des difficultés liées au recrutement des profils adéquats. Un chiffre interpellant est que 39% des CEOs déclarent diriger le changement vers une intégration du « big data » dans leur entreprise alors que seulement 9% des cadres dirigeants désignent le CEO comme le moteur du changement. Plus qu'un changement technique, il s'agit d'un changement profond du fonctionnement de l'organisation.

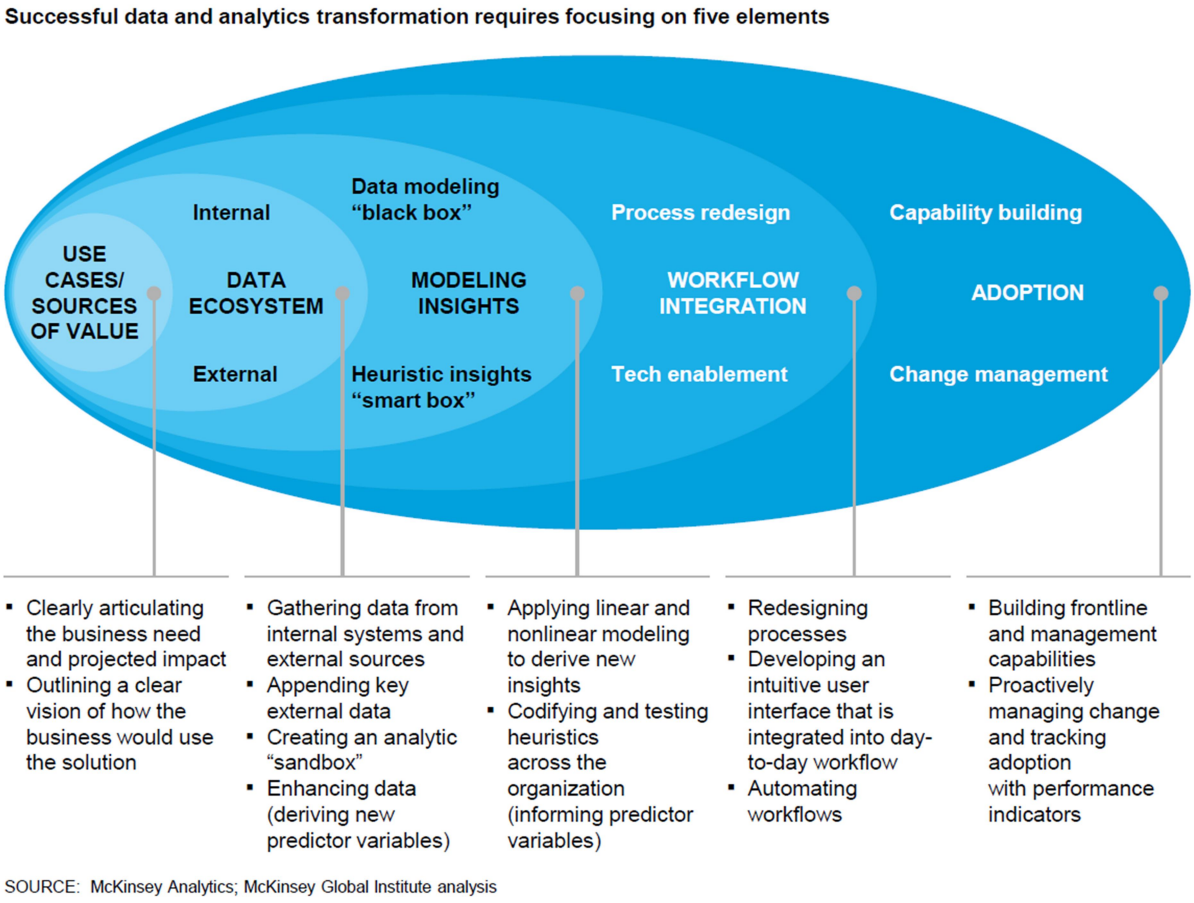

Figure 10. 5 étapes principales répertoriées par McKinsey pour effectuer les changements nécessaires au sein des entreprises désireuses d'intégrer les outils du « big data » dans leur processus de décisions [12]

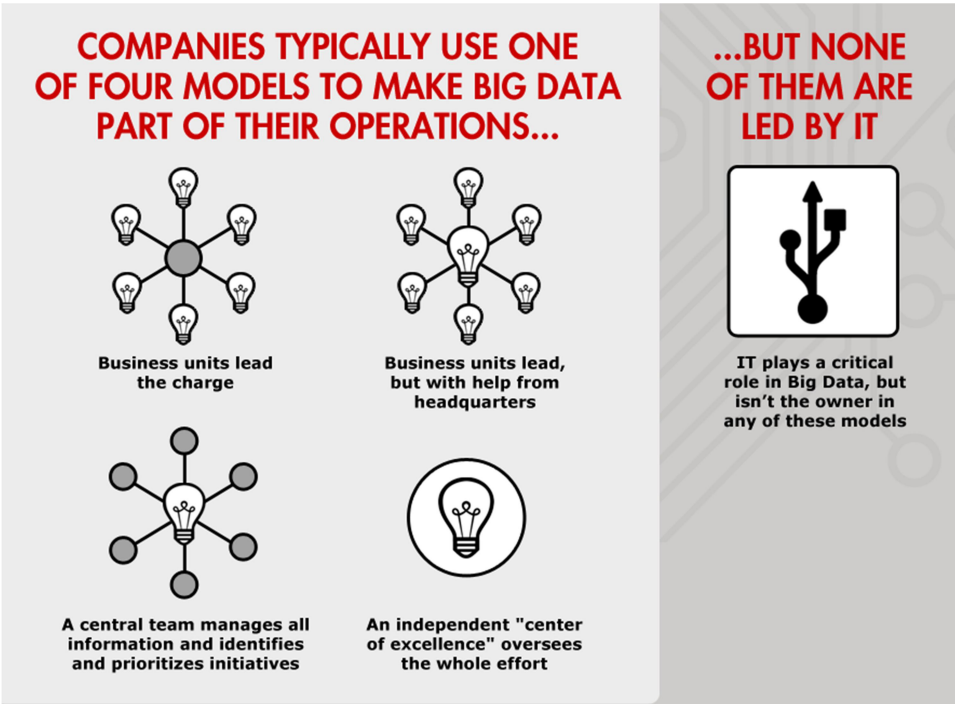

Figure 11. 4 types de changement d'organisation répertoriés par Bain&Company [7] pour intégrer le « big data » dans les processus des entreprises.

1.4. Amélioration des interactions avec le client

Les interactions entre les entreprises et les clients peuvent également bénéficier des informations recueillies au sujet des clients. Bain&Company [18] donne l'exemple des compagnies aériennes qui peuvent effectuer la corrélation entre l'identifiant de la personne qui les appelle, le numéro de vol et le statut du vol (ex : durée du délai). Sur base de cette analyse, ils peuvent avoir une idée de la raison pour laquelle leur client les appelle et ainsi fournir au plus vite une réponse appropriée.

De même, des techniques d'analyses pourraient être utilisées au début de la conversation téléphonique pour déterminer l'humeur du client et éventuellement rediriger l'appel vers un opérateur vers un opérateur formé pour gérer au mieux ce type de situations.

Comme nous pouvons le voir au travers de cet exemple, les données personnelles sont aussi susceptibles d'améliorer la qualité des échanges directs avec les clients.

1.5.Le Big Data à la portée de tous grâce aux outils de ciblage proposés par Facebook et Google

Dans un rapport commandé par Facebook, Deloitte [19] a quantifié l'impact de l'utilisation de Facebook sur l'économie mondiale. Les chiffres sont très impressionants, pour un coût de fonctionnement de l'ordre de 8 milliards de dollars, Facebook a généré une activité économique de 227 milliards de dollars et 4.5 millions d'emplois dans le monde (ces derniers chiffres ne prennent pas en compte l'activité de l'entreprise Facebook). Ces chiffres peuvent être divisés en trois grandes catégories

1. **Effets du marketing:** cette catégorie détermine l'impact sur les entreprises qui utilisent les pages Facebook et les outils de marketing de la plateforme pour entrer en contact avec leurs clients et développer leur image de marque ;
2. **Effets de plateforme:** impact sur l'économie associée au développement des applications smartphone qui intègrent des fonctionnalités associées à Facebook ;
3. **Effets de connectivité:** cette catégorie mesure l'influence de Facebook sur la vente de smartphones et les services associés tels que les forfaits mobiles.

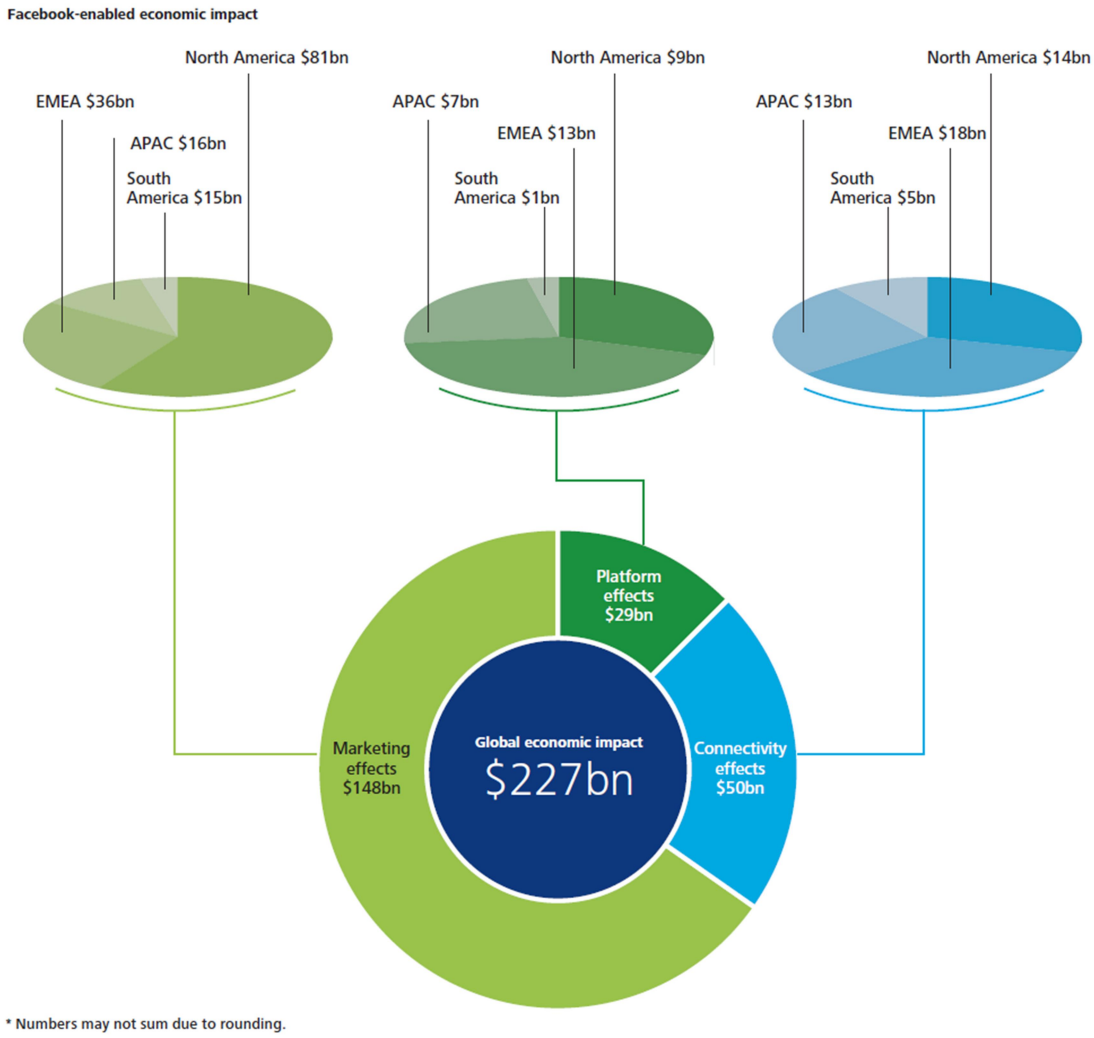

Figure 12. Représentation de l'impact économique lié à l'utilisation de Facebook à travers le monde en 2014 [19].

Dans son rapport, Deloitte indique que Facebook est une plateforme qui permet aux entreprises de s'adresser directement à leurs clients ou clients potentiels et qui a rendu plus accessible l'utilisation de la publicité ciblée à une large gamme d'entreprises. Grâce à l'application « *Facebook Ads* », il est possible de cibler différents groupes en fonction de leur âge, localisation, centres d'intérêts et de mesurer leurs réactions. L'effet le plus important est observé aux USA où 81 milliards de dollars et 870 000 emplois ont été générés en 2014 par les campagnes de marketing.

Des grandes entreprises comme Danone utilisent Facebook pour atteindre leur audience. Ces outils sont également accessibles à des PME et « *Start up* ». Les paragraphes ci-dessous décrivent deux success stories liées à l'utilisation de « *Facebook Ads* ».

1.5.1 Campagne de publicité pour Actimel [20]

Danone a collaboré avec Facebook pour segmenter le marché en 6 groupes distincts. Pour chacun de ces 6 groupes, Danone a créé une vidéo spécifique sur base des « *attitudes et valeurs culturelles* » de chacun des groupes afin de « faire appel aux goûts et aux centres d'intérêts de chacun des groupes ». Ces vidéos indiquaient la marque Actimel, étaient courtes et affichées de manière à pouvoir être visualisées sans son dans le fil d'actualité de chacun des prospects.

Cette campagne a touché 13 millions de personnes et Danone a pu mesurer un impact significatif auprès des femmes de 15 à 34 ans et une augmentation des ventes de 20% a été observée.

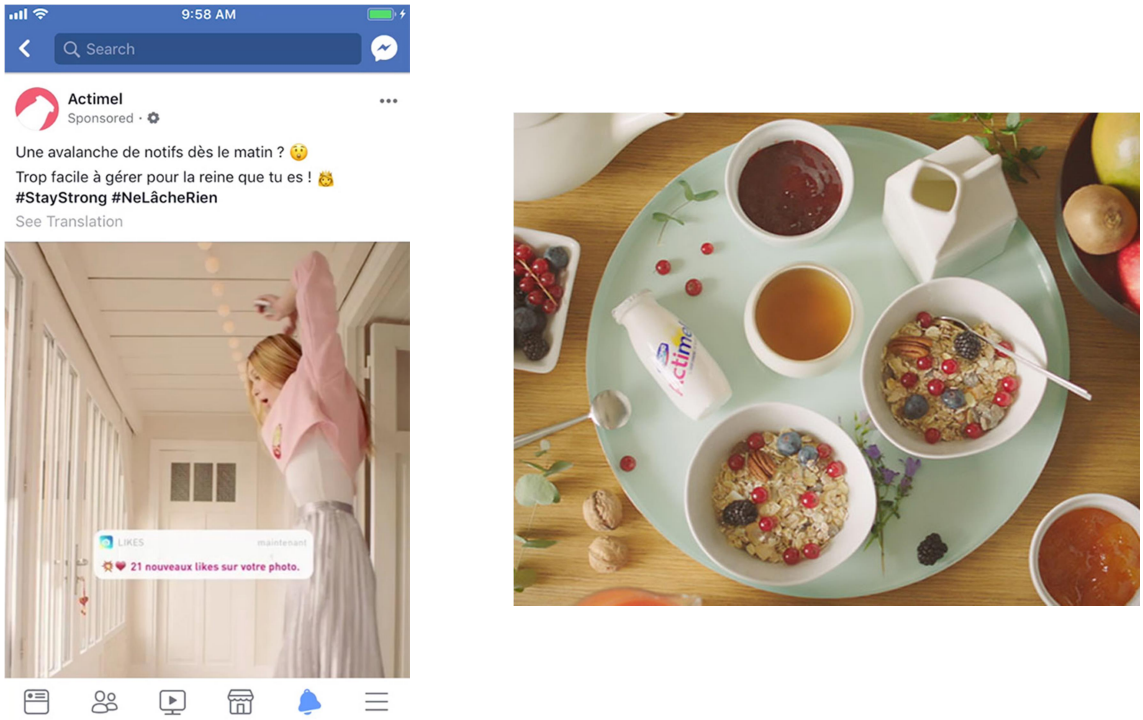

Figure 13. A gauche: capture d'écran d'une vidéo diffusée sur Facebook par Danone pour la promotion de son produit Actimel. A droite: une des images apparaissant dans la vidéo de promotion [20].

1.5.2 Campagne de publicité pour une jeune start up française – Prêt à pousser [21]

La jeune société française Prêt à pousser, crée en 2013, propose à ses clients de faire pousser des champignons, des herbes aromatiques ou encore des légumes dans leur cuisine.

L'objectif de l'entreprise était d'améliorer sa notoriété à l'approche des fêtes de fin d'année. Pour ce faire, elle a créé une vidéo (cf. Figure 14) présentant le produit et a ciblé une audience similaire à celle de ses clients existants.

Cette vidéo a été partagée massivement par les internautes, ceux-ci « *taguant* » leur contact Facebook pour attirer leur attention sur ce nouveau produit. Au terme de deux mois de campagne, les ventes ont augmenté aussi bien via internet que dans les points de ventes. La vidéo a généré 3.1 millions de vues, et 33% du trafic sur le site de vente en ligne de l'entreprise était issus des publicités diffusées sur Facebook.

Emma de Gélis, Responsable Marketing de l'entreprise indique que le choix de la vidéo sur Facebook avait pour but « *d'atteindre une audience très ciblée à moindre coût* » [21]. Cet exemple démontre bien que le « *big data* » est désormais à la portée de toutes les entreprises au travers des plateformes telles que Facebook et Google.

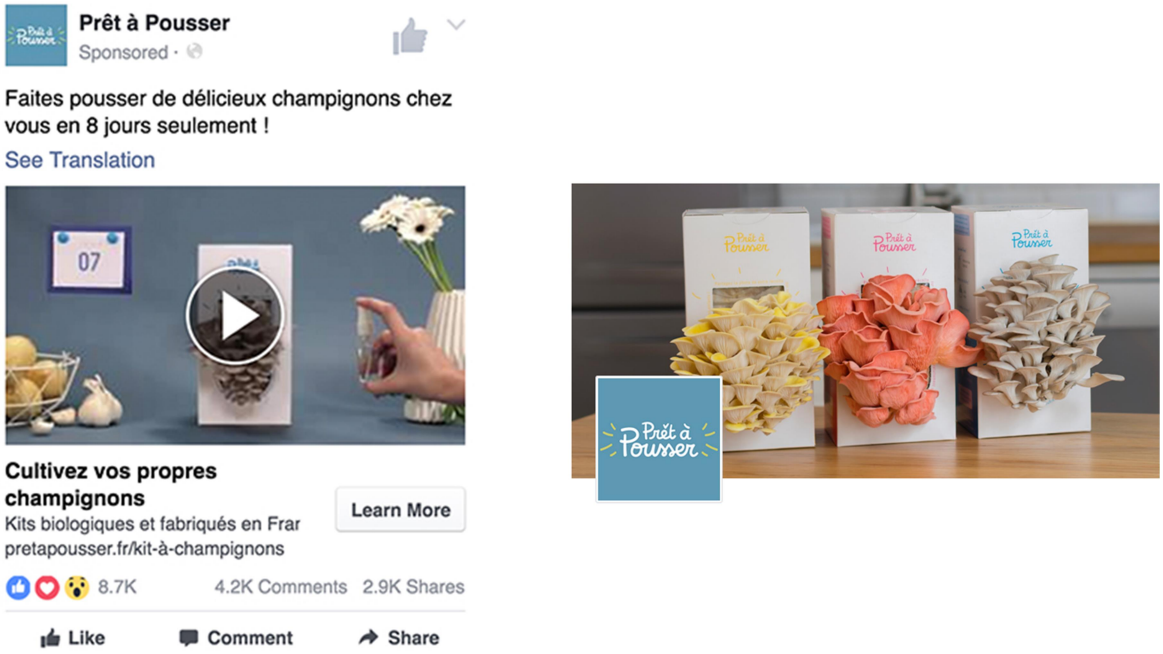

Figure 14. A gauche: Capture d'écran d'une vidéo de promotion d'un produit de la gamme « Prêt à pousser » diffusée sur Facebook. A droite: photos des produits mis en vente par la société « Prêt à pousser » [21].

Google a mis en place une plateforme appelée « *Google AdWords* » [22] qui permet de cibler de manière très précise des clients potentiels en fonction de leur âge, sexe, position géographique, centre d'intérêts, etc. et ce, à travers différents canaux (cf. Figure 15). Il peut s'agir d'annonces affichées dans le moteur de recherche lorsque la recherche d'un utilisateur de Google comprend des mots clés associés à l'annonce publicitaire. Il peut s'agir d'annonces graphiques affichées dans des pages web, des applications ou dans la messagerie « *Gmail* » ou encore d'annonces vidéos diffusées avant le lancement d'une vidéo disponible sur « *YouTube* ».

Google indique que grâce à cet outil, il est possible de toucher 90% des internautes dans le monde [22]. En outre, cet outil tout comme celui de Facebook, permet d'évaluer le succès de la campagne publicitaire et par la suite d'améliorer son contenu en fonction de ces résultats (cf. Figure 16).

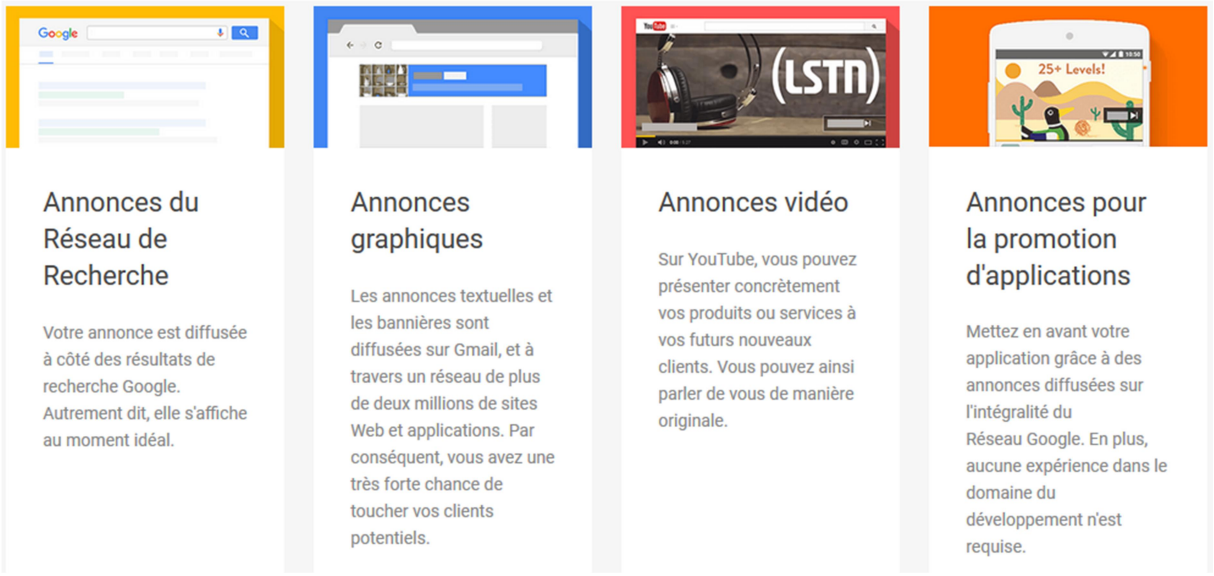

Figure 15. Illustration des différents canaux offerts par Google AdWords à ses clients pour la diffusion de leur contenu publicitaire [22].

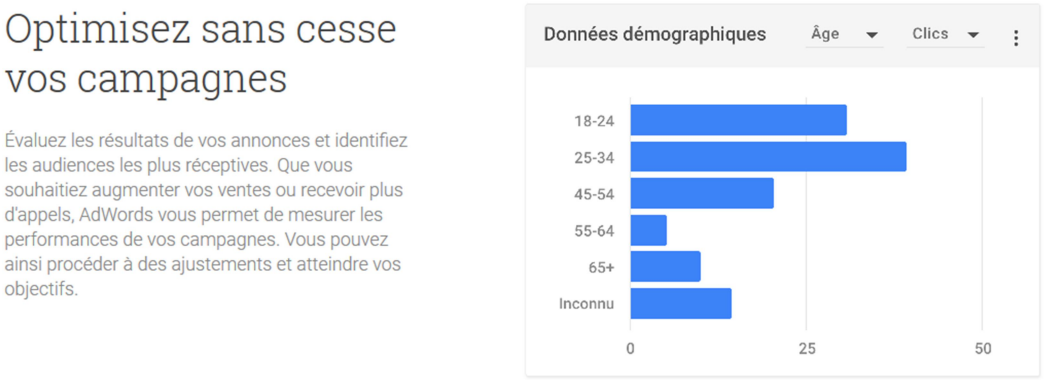

Figure 16. Graphique généré par « *Google AdWords* » montrant la répartition du nombre de « *clicks* » sur une annonce publicitaire par tranche d'âge [22].

Comme nous avons pu le voir au travers des exemples d'utilisation de Google et Facebook, le « big data » permet également de quantifier l'impact d'une campagne de marketing. On parle de « big data analytics ». Une étude effectuée en 2014 par McKinsey [23] auprès de 400 de ses clients indique que cette approche permet de réduire de 15 à 20% les dépenses liées au marketing. A budget constant, ces techniques permettent de tirer le maximum des dépenses en prenant de meilleures décisions. C'est par exemple le cas d'une société d'assurances de biens et risques divers basée aux USA qui a amélioré le retour sur investissement de ses dépenses marketing de 15% chaque année de 2009 à 2012.

1.6 Conclusions

Dans ce chapitre, nous avons décrit le grand champ d'application des techniques du « *Big Data* » et les gains considérables qu'une bonne utilisation de ces techniques peut avoir aussi bien pour les sociétés privées que pour les organismes publics. Nous avons vu que la transition vers l'implémentation de ces méthodes au sein des entreprises qui n'ont pas été construites autour de ces technologies demande plus qu'une simple mise à jour technique. En effet, l'achat de nouveau matériel informatique et l'engagement de personnel qualifié ne suffit pas. Il faut en outre une bonne intégration de ces nouvelles capabilités dans la structure de l'entreprise. Des formations doivent être données au personnel qui utilisera effectivement les résultats des analyses du traitement de données et ce, dans le but de lui permettre de bien comprendre les principes des méthodes employées et les résultats générés. Enfin, la transition vers l'utilisation du « big data » doit être pilotée par le CEO.

La dernière partie de ce chapitre a montré que l'utilisation des techniques du « big data » à des fins de marketing peut se faire par l'intermédiaire de plateformes telles que Facebook et Google qui permettent de toucher une large audience, de segmenter le marché sur base des centres d'intérêts, de la localisation géographique, de l'âge, etc. et de mesurer l'impact des campagnes marketing sur chacun des segments ciblés.

Il ressort de ces exemples, des bénéfices pour les entreprises qui peuvent toucher une large audience, cibler chacun des segments de manière adéquate, et ainsi optimiser le retour sur investissement des dépenses associées au marketing. En outre, il est possible de collecter le feedback des consommateurs par rapport au lancement de nouveaux produits, mieux cerner leurs attentes et par la suite guider les efforts de recherches et développements pour les produits futurs. Les clients de leur côté se voient proposer des publicités et des offres qui correspondent davantage à leurs attentes et peuvent interagir plus facilement avec les marques.

Cette situation idéale où entreprises et clients tirent mutuellement un bénéfice de ces nouvelles méthodes n'est que la partie émergée de l'iceberg. Les données utilisées pour nous cibler peuvent être très personnelles, peuvent être parfois collectées à notre insu et peuvent présenter le risque d'être utilisées au détriment des consommateurs dans le futur. Ces dérives possibles sont décrites dans le chapitre suivant au moyen d'exemples de situations réelles qui se sont présentées il y a au plus quelques années.

Chapitre 2 – Inconvénients, risques et dangers associés à l'utilisation des données collectées

2.1.Introduction

En février 2018, le tribunal de première instance de Bruxelles a rendu un jugement dans l'affaire opposant la commission de la vie privée belge au groupe Facebook [24, 25]. Lors de ce jugement, Facebook a été condamné pour non-respect de la loi belge sur la protection des données. Concrètement, le juge reproche à Facebook de « *collecter des informations personnelles de manière disproportionnée et sans consentement, non seulement des internautes qui sont inscrits à son service mais également de tous les non membres qui cliquent sur le bouton « j'aime » comme ceux que l'on trouve sur des millions de sites web dans le monde* » [24].

En pratique, Facebook a mis au point une méthode de collecte de données sur les personnes non-membres du réseau social : lorsqu'un internaute visite une page web dotée d'un bouton « j'aime », Facebook collecte cette information et l'enregistre dans un profil lié à l'internaute. En outre, pour les pages ne disposant pas de bouton « j'aime » Facebook fait appel à des pixels, à savoir des images présentes sur des pages webs et invisibles pour l'utilisateur, pour pouvoir collecter des informations. Le tribunal estime que cette collecte massive de données ne se justifie pas et que les utilisateurs ne sont pas suffisamment informés et n'ont pas donné leur accord pour ce type de pratiques.

Figure 1. Caricature de Kroll sur le jugement rendu par le tribunal de première instance de Bruxelles à l'encontre de Facebook [24].

Facebook n'est évidemment pas la seule application à collecter des données au sujet de ses utilisateurs. Dans ce chapitre, nous allons discuter des dérives associées à la collecte de nos données. Pour ce faire, nous présenterons des exemples récents parus dans la presse ou sur internet. Ceux-ci concernent notamment un centre commercial français qui collecte des informations sur ses clients grâce à leur connexion wi-fi (cf. paragraphe **Erreur ! Source du renvoi introuvable.**), des objets connectés non suffisamment sécurisés (cf. paragraphe 2.3) ainsi que l'utilisation de nos données des partis politiques (cf. paragraphe 2.4) et par des compagnies d'assurances (cf. paragraphe 2.5)

2.2.Données collectées à notre insu via notre smartphone

Dans le courant de l'année 2017, le site d'information L'express/L'expansion [26-27] indiquait que deux centres commerciaux français : les Quatre Temps et le BHV, tous deux situés à Paris, récoltaient des données au sujet de leurs clients lors de leur connexion sur le réseau Wi-fi accessible au sein des commerces.

Le but des centres commerciaux est d'obtenir des informations sur le temps passé dans les différentes boutiques, géo-localiser les clients dans les rayons, déterminer les habitudes d'achats, etc. Ces pratiques ont interpellé certains consommateurs qui en ont fait état sur Twitter comme le montre les deux photos répertoriées sur la Figure 3.

Ce procédé n'est pas contraire au droit français pour autant que les règles suivantes soient respectées [27]:

- le fait que des données sont collectées doit clairement être mentionné aux clients;
- les informations collectées ne doivent pas pouvoir être reliées aux clients, elles doivent être anonymisées;
- les données doivent être supprimées dès que leur propriétaire sort du centre commercial.

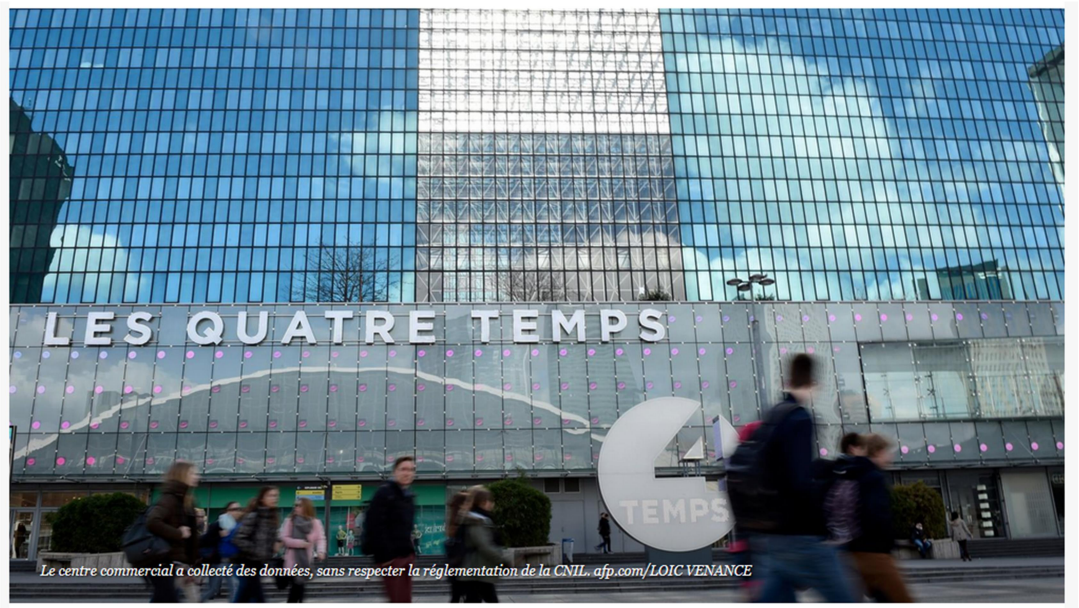

Figure 2. Photo du centre commercial « Les Quatre Temps » à Paris qui utilisait en 2017 son réseau Wifi pour collecter des données au sujet de ses clients [26].

Ces règles ne sont pas toutes respectées puisque les centres commerciaux font état d'un délai de conservation des informations de 6 mois. En outre, ces données sont associées à l'adresse MAC du smartphone qui est un identifiant unique.

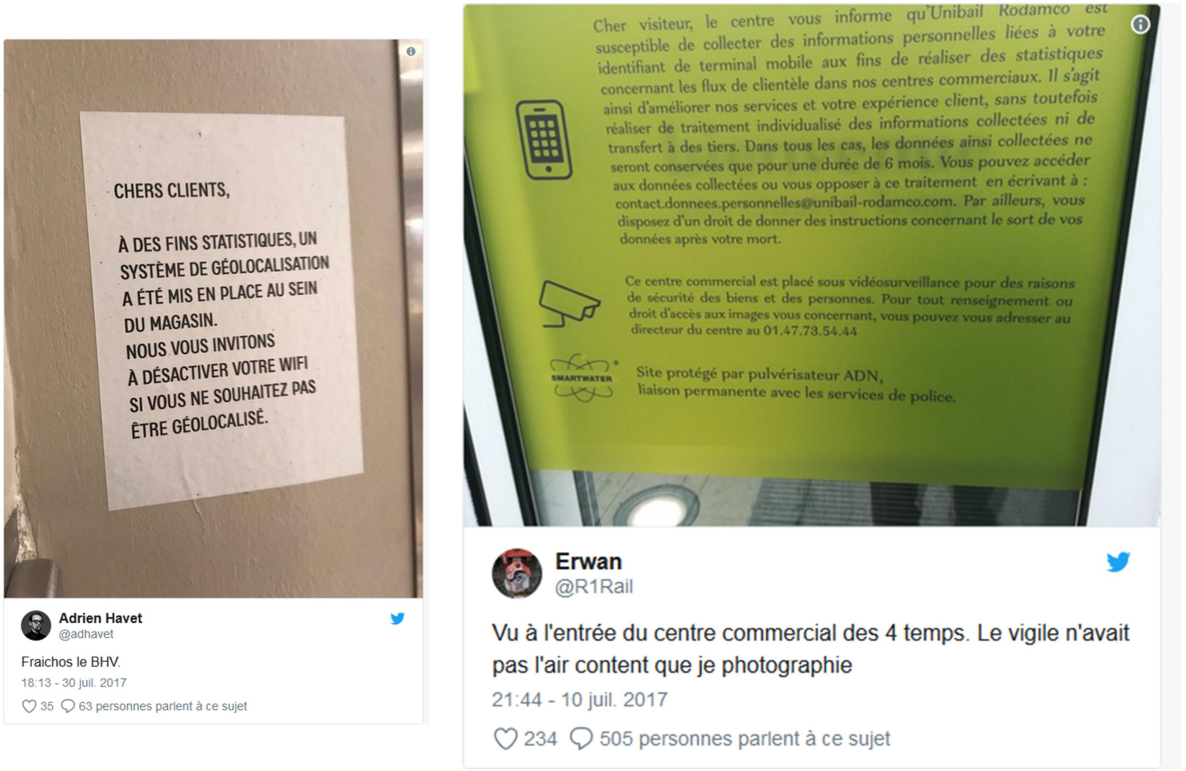

Figure 3. Photos des affiches présentes respectivement au centre commerical « BHV » situé à Paris (à gauche) et au centre commerical « les Quatre Temps » (à droite) informant les clients de l'utilisation du réseau Wifi pour collecter des données à leur sujet [27].

Le deuxième exemple évoqué dans ce chapitre fait écho à un article du journal le Monde « *Izly, l'appli du Cnous qui géolocalise des étudiants et renseigne des sociétés publicitaires* » [28]. Celui-ci concerne une application de paiement mobile appelée « *Izly* » développée suite à une initiative du Centre national des œuvres universitaires et scolaires (Cnous) dans le but de permettre aux étudiants de payer leurs repas dans les restaurants universitaires. L'objectif du Cnous étant de réduire le nombre de paiements en liquide et de diminuer le temps d'attente aux caisses. De plus, certains centres universitaires permettent le payement de photocopies ou l'accès à différents bâtiments au moyen de cette application. En 2017, un étudiant en informatique de l'Ecole Normale Supérieure de Lyon constate que ses coordonnées GPS sont utilisées par l'application. Il contacte alors le journal le Monde qui investigue le sujet [28].

Les journalistes du Monde constatent tout d'abord que les données GPS sont bien envoyées à des tiers par l'application « Izly » (cf. Figure 4Figure 5). Ils ont ensuite listé les différents intervenants par lesquels les données transitent.

La figure 5 montre le transfert de données entre l'application « *Izly* » et des tiers : « *Neerby* » reçoit les informations provenant de « *Izly* », elle transmet alors la position à « *Take&Buy* ». A son tour, « *Take&Buy* » transmet cette information à des annonceurs. Les annonceurs approuvés au préalable par le « *Cnous* » peuvent alors envoyer aux utilisateurs de l'application des messages publicitaires par l'intermédiaire de « *Take&Buy* ».

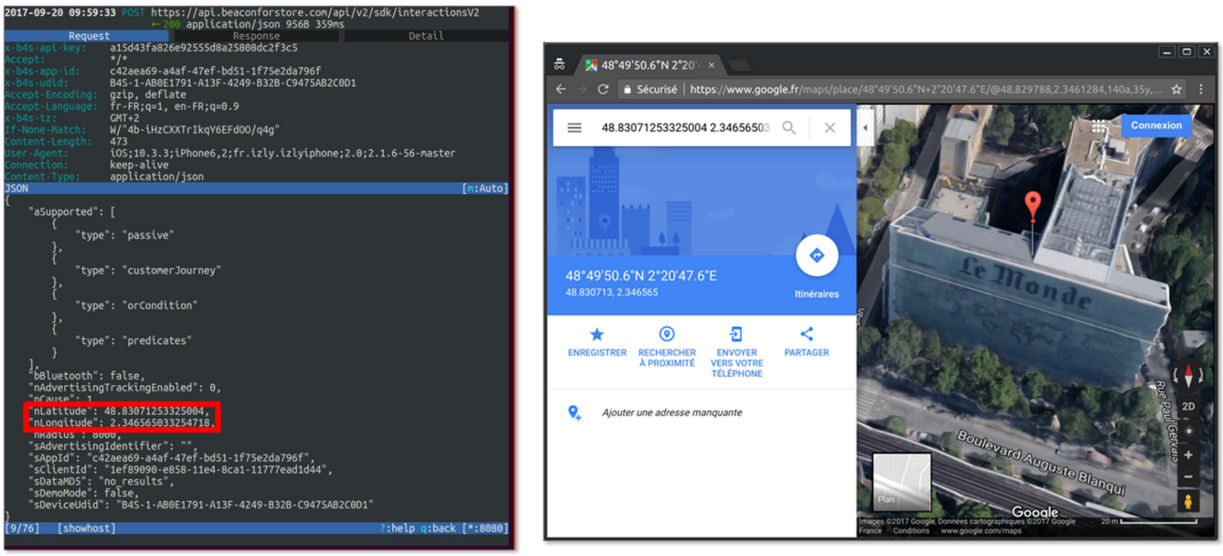

Figure 4. La figure de gauche montre les données envoyées par l'application « Izly » ; les coordonnées GPS de l'utilisateur sont entourées en rouge. La figure de droite montre que les coordonnées GPS récoltées par l'application correspondent bien au siège du journal Le Monde, où l'application a été testée par les journalistes [28].

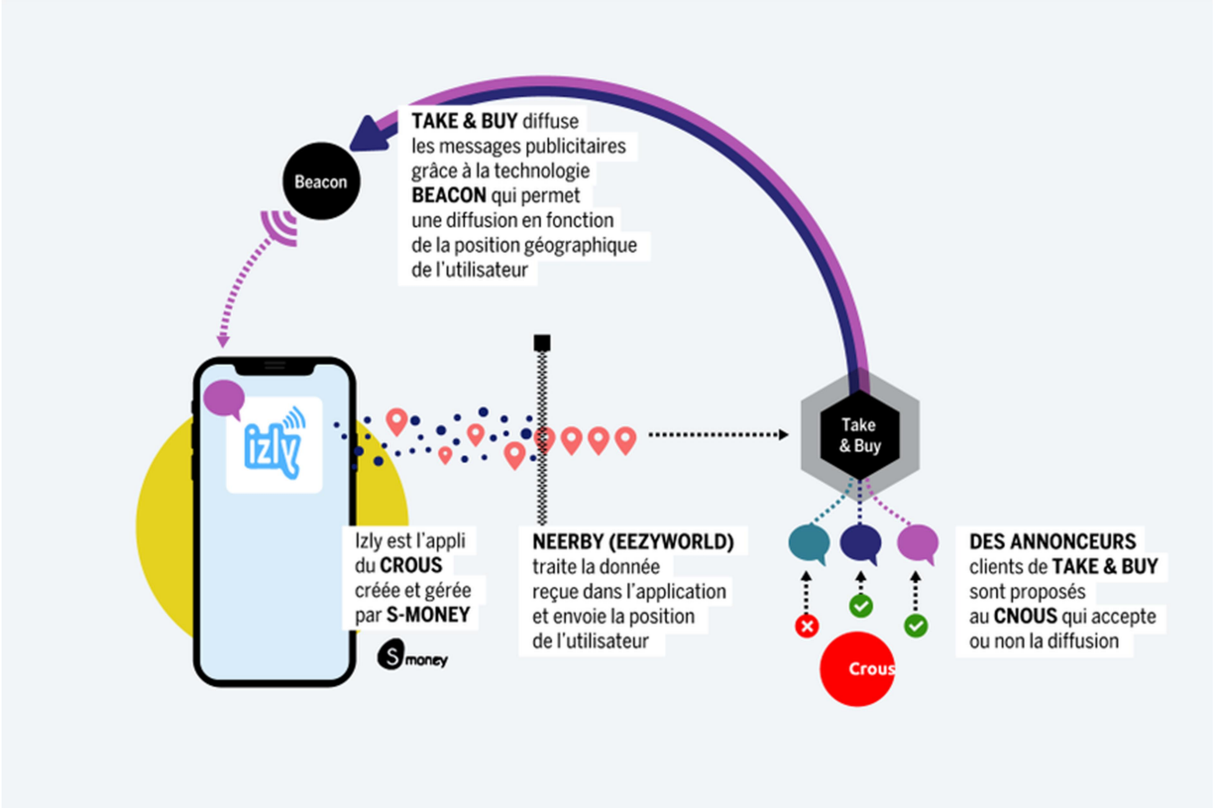

Figure 5. Schéma illustrant l'échange d'informations entre l'application de paiement « *Izly* » et des sociétés partenaires : « *Neerby* » reçoit les informations provenant de « *Izly* », elle transmert alors la position à « *Take&Buy* » qui à son tour les transmet à des annonceurs. Les annonceurs approuvés au préalable par le « *Cnous* » peuvent alors transmettre aux utilisateurs de l'application des notifications publicitaires par l'intermédiaire de « *Take&Buy* » [28].

L'avantage de l'envoi de notifications publicitaires est évidemment de permettre de couvrir une partie des frais de fonctionnement de l'application. L'autre partie étant financée par le prélèvement d'un pourcentage sur les paiements effectués au moyen de l'application.

C'est le manque de transparence au sujet des données échangées qui pose question dans cet exemple. En effet, même si les conditions générales d'utilisation de l'application indiquent l'utilisation de la géolocalisation par l'application, « *combien d'étudiants savaient-ils comment ces données étaient réellement utilisées et quelles étaient les entreprises qui les recevaient ?* » [28].

En outre, toujours selon Le Monde « *Il faut se pencher sur les quelques lignes d'une autre version des conditions d'utilisation du service, très loin d'être lues par la majorité des étudiants, pour savoir que les données personnelles de l'utilisateur sont recueillies par « S-money, le groupe BPCE, ainsi [que par] ses filiales directes et indirectes ou [par] ses partenaires commerciaux » et peuvent être utilisées pour de la « prospection et [de] l'animation commerciale* » » [28].

C'est ce manque de transparence qui a conduit des étudiants à s'interroger sur les implications que cela pourrait avoir au sujet de leur vie privée. Suite à la parution de l'article du Monde, le « Cnous » a décidé de supprimer l'utilisation des données GPS par l'application « Izly » et ce pour éviter toute ambiguïté et toute inquiétude.

Ce troisième exemple fait plutôt référence à l'insouciance voire à la négligence des utilisateurs d'applications par rapport aux données qu'ils partagent. Deux articles parus début 2018 : « *Une appli sportive dévoile les bases militaires américaines en Syrie et en Irak* » [29] et « *Géolocalisation et appli sportive: l'armée française rappelle ses troupes à l'ordre* » [30] révèlent que des membres de l'armée française et américaine ont utilisé l'application Strava dans le cadre de leurs entrainements physiques en Irak, Afghanistan et au Niger.

Strava est une application qui permet à ses utilisateurs d'enregistrer le chemin parcouru lors de leurs entrainements de course à pieds, à vélo, etc. et ensuite de partager ces informations avec d'autres utilisateurs de l'application. Cette application, parfois appelée le « *Facebook des sportifs* », montre le déplacement de ses utilisateurs à travers le monde. Dans des pays comme ceux cités précédemment, l'application est très peu utilisée par la population locale. Dès lors, les déplacements affichés dans ces régions correspondent presque exclusivement à des itinéraires empruntés par des soldats dans le cadre de leurs opérations (cf. Figure 6).

Ces deux articles indiquent qu'aucune base militaire secrète n'a été dévoilée par cette application; elles étaient en effet connues de la population locale. Cependant, les informations partagées montrent la fréquence des déplacements effectuées dans la zone et pourraient faciliter certaines attaques. Ce phénomène est désormais pris très au sérieux par les responsables de la défense française via notamment la publication d'un « Guide de bon usage des réseaux sociaux » [30].

Figure 6. Tweet d'une capture d'écran de l'application « *Strava* » montrant l'itinéraire suivi par des membres de l'armée française au Niger dans le cadre de leurs opérations [30].

2.3.Données collectées via les objets connectés de nos maisons

Nous l'avons vu dans les paragraphes précédents, les applications de nos smartphones collectent des informations nous concernant, parfois à notre insu. C'est aussi le cas des objets connectés, ceux-ci disposent de moyens de communication comme le Wi-Fi, 4G, Bluetooth, etc. Parmi ces objets on peut citer par exemple, les podomètres, les montres connectées mais aussi des objets liés à nos maisons tels que thermostats, frigos, ampoules, onduleur de panneaux photovoltaïques [31]. Les données récoltées par ces différents appareils peuvent être consultées à tout moment via une application ou sur le site internet du fabricant.

En mai 2018, Test-Achats, l'organisme de défense des consommateurs en Belgique a publié les résultats d'une enquête sur la sécurité des objets connectés [32-33]. Dans cette étude, ils ont fait appel à deux hackers éthiques de la société britannique SureCloud et leur ont demandé de hacker un maximum d'objets connectés parmi les 19 installés dans une maison en vue du test. Verdict, en 5 jours, ils sont parvenus à prendre le contrôle ou intercepter des données issues de près de la moitié des appareils. Les objets qu'il a été possible de pirater ne sont pourtant pas anodins: une serrure connectée qu'il est possible de déverrouiller via smartphone a pu être ouverte à distance par les hackers. Un autre exemple, un système d'alarme composé d'une caméra de capteurs de mouvements et d'un détecteur de fumée a pu lui aussi être contrôlé par les hackers ; ils ont capté les images de la caméra de surveillance et ont pu désactiver les différents capteurs. Une montre GPS pour enfant qui permet aux parents de localiser à tout moment leur enfant et de communiquer avec lui via messages vocaux a été elle aussi piratée ; les messages vocaux ont été interceptés ainsi que la position de l'enfant. Dernier exemple, une tablette pour enfant ; les hackers ont pris le contrôle de la caméra et ont écouté les conversations privées via le micro de l'appareil.

Figure 7. Objets connectés utilisés dans lors des tests effectués par Tests-Achats en 2018 [32-33]. A gauche : une serrure connectée qu'il est possible de déverrouiller grâce à son smartphone. Au centre : une montre connectée pour enfant indiquant sa position GPS. A droite : une tablette pour enfant.

Ce manque de protection est assez interpellant. Déjà en 2014, une enquête réalisée par « *HP Security Research* » sur 10 appareils connectés a montré des résultats inquiétants pour la vie privée et la sécurité des utilisateurs de ces objets [34] (cf. Figure 8) :

- 80% des objets testés collectaient des informations privées telles que l'adresse, date de naissance voire même des informations bancaires telles que les données de cartes de crédits ;
- 70% des objets faisaient transiter des informations de manière non cryptée sur le réseau local ;
- 80% ne nécessitaient pas de mot de passe suffisamment complexe pour garantir la sécurité des données des utilisateurs ;
- 60% ont montré des signes de vulnérabilité au travers de leur interface web ;
- 60% n'utilisaient pas une connexion sécurité en téléchargeant des mises à jours logicielles.

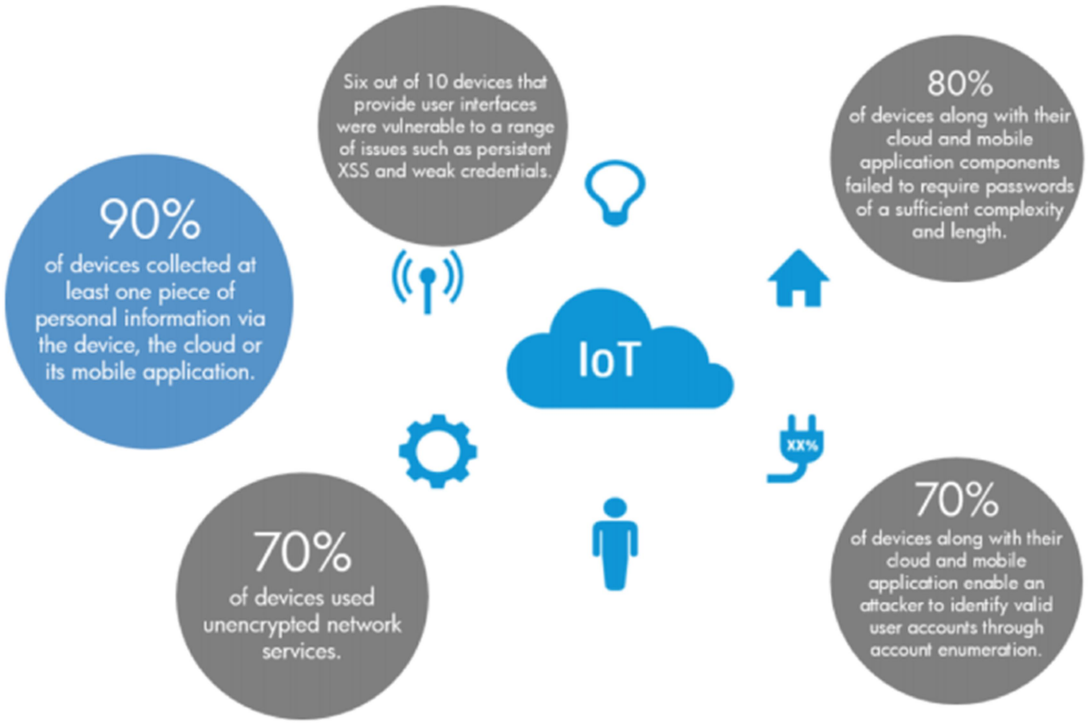

Figure 8. Résumé des failles de sécurité observées par « *HP Security Research* » lors de tests effectués sur 10 objets connectés en 2014 [34].

Il existe désormais des jouets pour enfants connectés à internet. C'est pas exemple le cas de la poupée « *Cayla* » et du robot « *i-Que* » (cf. Figure 9) tous deux fabriqués par la société « *Genesis Industries* » basée à Hong-Kong. En décembre 2017, cette société a été mise en demeure par la Commission nationale de l'informatique et des libertés (Cnil) pour « *atteinte grave à la vie privée en raison d'un défaut de sécurité* » [35].

En effet, « *des vérifications ont permis de relever que la société collecte une multitude d'informations personnelles sur les enfants et leur entourage : les voix, le contenu des conversations échangées avec les jouets (qui peut révéler des données comme une adresse, un nom,…) mais également des informations renseignées dans un formulaire* » [35].

Figure 9. A gauche : photo de la poupée connectée « *Cayla* ». A droite : photo du robot connecté « *i-Que* ». Ces deux jouets produits par l'entreprise « *Genesis Industries* » [35]

Un des problèmes de sécurité pour ces deux jouets est lié à l'absence de sécurisation de la connexion bluetooth ; n'importe qui dans un rayon de 9 mètres peut se connecter à ses jouets grâce à un smartphone par exemple et ainsi communiquer avec les enfants au travers du jouet.

Un autre problème relevé par la Cnil : « *les propriétaires ne sont pas informés du fait que la société transfère des contenus de conversations auprès d'un prestataire de service situé hors de l'Union européenne* » [35].

L'article du Figaro relate également deux autres failles de sécurité : en 2015, un hacker a pu se procurer 5 millions de données personnelles de parents et de 6 millions d'enfants propriétaires de jouets fabriqués par la société *VTech*. En 2017, les jouets produits par « *Spiral toys* » ont rendu accessibles plus de 200 000 enregistrements vocaux d'enfants [35].

Dernier exemple de cette section, le téléviseur connecté produit par la société américaine « *Vizio* », collectait des données relatives aux contenus affichés sur son écran. Ces informations ainsi que des données du type : âge, sexe, niveau de revenu, niveau d'éducation, taille du ménage, etc. étaient transmises à des sociétés de ciblage qui proposaient alors sur les ordinateurs et tablettes du ménage des publicités ciblées sur base du contenu visionné [36].

La société qui détenait en 2016, près de 20% du marché aux Etats-Unis a été condamnée à payer 2.2 millions de dollars pour cette affaire qui concerne 11 millions de téléviseurs [36].

2.4.Utilisation des données personnelles lors des campagnes électorales

Nos données personnelles sont également utilisées par des partis politiques lors des campagnes électorales. C'est ce que révèle une enquête du journal « *Le Soir* » parue en avril 2018 [37].

Tous les partis politiques belges ont désormais intégré les réseaux sociaux dans leur stratégie de communication. Les plus avancés sont au nord du pays, avec la N-VA qui a fait appel à la société de marketing « *Brandhome* » pour sa campagne de 2014. Le CD&V a récemment refait son retard en la matière en utilisant Facebook pour cibler les électeurs du SP.A, de Groen et de la N-VA avec des thèmes bien précis pour chacun d'eux.

Le PTB quant à lui utilise le logiciel « *Nation Builder* », cette plateforme qui prend la forme d'un site internet. Celui-ci permet de construire une base de données rassemblant des informations sur les militants. Celles-ci proviennent des formulaires remplis lors de l'inscription sur le site croisées avec des données partagées précédemment sur Facebook ou sur d'autres réseaux sociaux par chacun des utilisateurs.

Sur base de ces informations, le parti ou les candidats peuvent alors communiquer des messages ciblés vers leurs militants et électeurs potentiels via des SMS, tweets, messages laissés sur les messageries vocales, e-mails, posts Facebook, etc. [37]. « *Nation Builder* » a également été utilisée par Emmanuel Macron, Jean-Luc Mélenchon, Donald Trump lors des dernières élections auxquelles ils ont participé [38].

Un article du monde de Février 2018 [39], indique que Facebook aurait été utilisé par un groupe russe, appelé « *Internet Research Agency* » (IRA), spécialisé dans la propagande sur Internet. Son rôle était de de créer de faux comptes sur différents réseaux sociaux et de traiter des sujets liés à la religion, l'immigration ainsi qu'à la place des afro-américains dans la société américaine. Ces comptes devaient également servir à propager des rumeurs au détriment d'Hilary Clinton et d'autres candidats à l'exception de Donald Trump et Bernie Sanders. Ce groupe a également organisé des manifestations sur le sol américain en faveur de Donald Trump, là aussi, des évènements dont la promotion était assurée grâce aux réseaux sociaux. Le document d'inculpation de la justice américaine cité par le journal Le Monde indique d'ailleurs que l'IRA, « *n'a fait qu'utiliser des outils conçus pour le marketing et la publicité* » [39].

La société Cambridge Analytica est quant à elle accusée d'avoir utilisé les données de 87 millions d'utilisateurs Facebook [37] sans leur consentement dans le cadre de la campagne présidentielle américaine. Cette société qui cherche à utiliser les « *caractéristiques psychologiques des électeurs pour les influencer* » [40] a pour ce faire fait appel à Aleksandr Kogan, un chercheur à l'université de Cambridge. Ce dernier a créé une application Facebook « *thisisyourdigitallife* » grâce à laquelle, des internautes peuvent remplir un questionnaire psychologique contre rémunération. Outre ces réponses, l'application collecte un grand nombre de données associées au compte Facebook des répondants mais aussi de leurs contacts sur le réseau social. Ces infirmations ont été utilisées par les équipes de campagne de Donald Trump pour les aider à cibler leur message électoral [40].

Dans une interview accordée au quotidien Libération *[41]*, Christopher Wylie, l'ancien directeur de recherche chez Cambridge Analytica, indique que cette entreprise a également été impliquée dans le référendum sur le Brexit : « *cela a joué un rôle crucial* ». Il indique en outre que les activités de l'entreprise s'étendaient également à *« la collecte privée de renseignements, pour collecter de quoi compromettre une opposition. » [41].*

2.5.Utilisation des données collectées par les compagnies d'assurances

Un autre champ d'application des données privées est le domaine des assurances. Le Boston Consulting Group a identifié les différents éléments de la chaine de valeur du monde de l'assurance qui pourrait bénéficier de l'utilisation du « *Big Data* » [42], ces éléments sont représentés sur la Figure 10.

BCG classe ces différents domaines en deux catégories : ceux qui pourraient bénéficier d'une amélioration comme la détection de la fraude et la prévention des risques et ceux qui pourraient subir un changement plus important (une « *révolution* ») comme l'évaluation des risques.

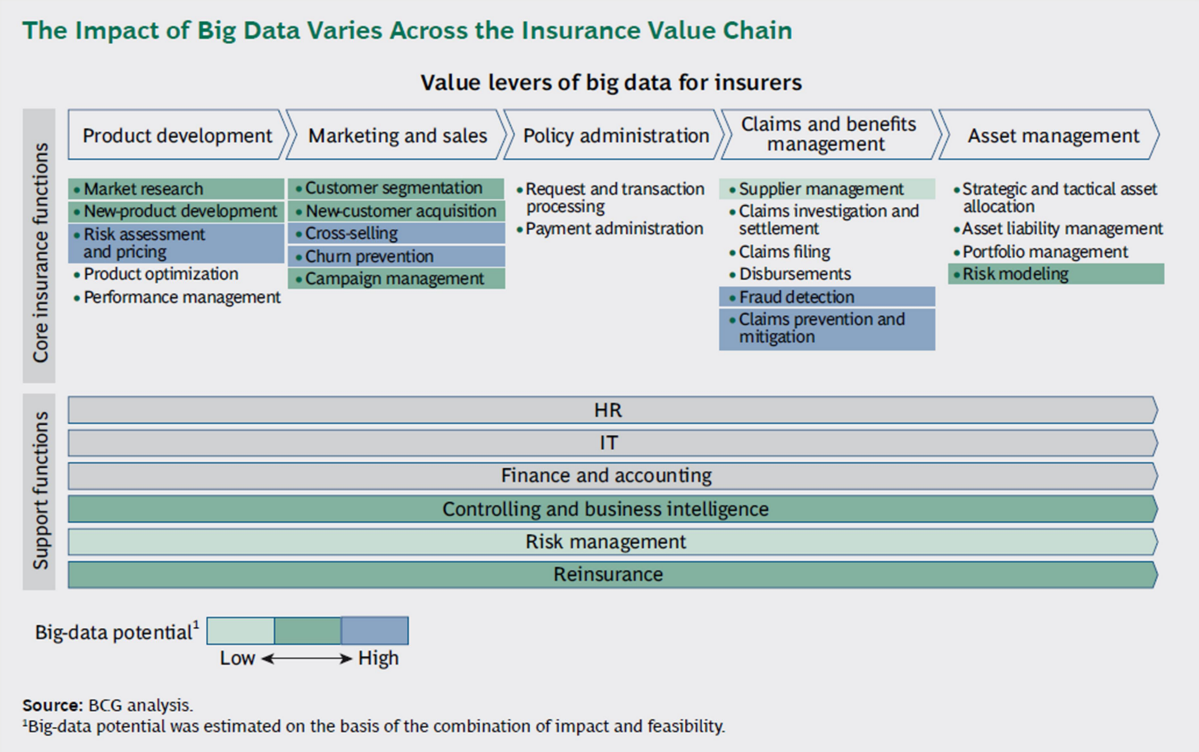

Figure 10. Impact de l'utilisation des techniques de « *Big Data* » dans la chaine de valeur des assureurs [42]

Dans le cas de la détection des fraudes, pour un accident de voiture par exemple, une approche « Big Data » engendrerait trois enquêtes distinctes. La première aurait pour but de détecter un éventuel schéma frauduleux : est-ce que les dommages du véhicule, les conclusions du médecin corroborent la version de l'assuré. La deuxième se rapporterait au passé de l'assuré : quelle est sa situation financière, a-t-il des antécédents criminels, a-t-il eu un comportement suspicieux en ligne, sur les réseaux sociaux, etc. La troisième, l'assuré a-t-il un lien avec des personnes impliquées dans des accidents qui paraissaient suspicieux ou des personnes impliquées dans des activités suspectes [42].

BCG indique qu'un assureur basé en Amérique du Nord a déjà mis en place ce type de méthodologie pour évaluer les sinistres autos. Cela lui a permis d'augmenter son taux de détection des fraudes de 30% conduisant à une réduction de 2 à 3% du montant total remboursé aux assurés. Ce type de d'approche a permis de réduire la durée nécessaire aux enquêtes des assureurs conduisant à un remboursement plus rapide et ainsi une meilleure satisfaction du client. Sans parler d'une réduction du nombre de tâches manuelles [42].

Un des aspects révolutionnaires du « *Big Data* » pour les assurances concerne l'évaluation du risque pour l'assuré en temps réel. Ainsi, il serait possible aux assureurs d'offrir à leurs clients des « one-time insurance » pour des activités de courte durée telles que le ski, le vélo, etc. En arrivant sur le lieu de son activité l'assuré pourrait souscrire à une assurance pour une durée limitée à l'aide de son smartphone par exemple. La prime pourrait être calculée sur base de l'activité pratiquée évidemment mais aussi des conditions locales, températures, conditions météorologiques, etc. Ainsi, l'assureur peut offrir à ses clients un service personnalisé. Un autre exemple de personnalisation concerne les assurances pour voiture basées sur le kilométrage parcouru et les données GPS telles que la vitesse et le mouvement du véhicule. Le risque serait dès lors évalué sur base du style de conduite [42].

Ce type de nouvelles offres soulève de nombreuses questions. Avec une telle personnalisation des offres, sera-t-il possible à un conducteur ayant déjà eu plusieurs accidents sérieux de trouver une assurance abordable ? La même question se pose si les données liées à nos habitudes de vie (type de sport pratiqué, loisirs, type d'alimentation, nombre de restaurants visités chaque mois, etc.) sont utilisées pour déterminer le montant des assurances. Pire, qu'en sera-t-il pour les personnes ayant souffert par le passé d'une maladie grave, un cancer par exemple. Cet exemple montre une fois encore que les techniques de « *Big Data* » peuvent apporter du changement positif mais aussi pas mal de questions.

2.6.Conclusions

Dans ce chapitre, nous avons passé en revue la face un peu plus sombre associée aux collectes de données via les sites internet que nous visitons, les applications smartphones ainsi que les objets connectés de plus en plus présents dans nos maisons. Toutes ces données peuvent par exemple être utilisées de manière abusive pour essayer d'influencer l'opinion avant une élection comme cela a par exemple été le cas dans la présidentielle américaine ou le référendum sur le Brexit. Demain, ces données pourraient également être utilisées par les assurances pour évaluer le montant des primes par exemple.

Une utilisation abusive des données est à éviter à tout prix. En effet, une étude du Boston Consulting Group, a montré qu'une mauvaise utilisation des données par les entreprises pourrait conduire à une réduction de chiffre d'affaires de 5 à 8% après la première année. Cette diminution pourrait se réduire et passer de 3 à 5% au cours de la deuxième année. De plus, en brisant la confiance avec les consommateurs, ces entreprises se priveraient d'une quantité significative de données. Cette étude indique également que le nombre de personnes sensibles à une mauvaise utilisation de leurs données va augmenter dans le futur [43]. Il est dès lors important de prendre les mesures nécessaires pour créer et conserver un lien de confiance avec les consommateurs.

Chapitre 3. Les règles en vigueur en Europe relatives à la collecte de données personnelles

Le but de ce chapitre est de décrire très brièvement les grands principes du nouveau Règlement Général sur la Protection des Données (RGPD). Ce règlement [44] qui comporte 99 articles est entré en vigueur le 25 mai 2018 et encadre la collecte ainsi que le traitement effectué par les sociétés et institutions de nos données personnelles [45].

Par donnée personnelle on entend toute information se rapportant à une personne physique et susceptible de l'identifier de manière directe ou indirecte. Il peut s'agir par exemple du nom, d'un identifiant, d'une photo, du numéro de sécurité sociale, d'une plaque d'immatriculation, d'une adresse postale, d'une adresse e-mail, d'un numéro de téléphone, de données de localisation, d'un identifiant en ligne comme une adresse IP, etc. [46]

Ce texte protège l'ensemble des résidents européens et doit être respecté par toutes les entreprises privées ou publiques qui proposent des biens et services sur le marché de l'Union Européenne ou qui collecte et utilisent des données personnelles relatives à des résidents de l'UE [47].

Ces nouvelles règles reposent sur 4 grands principes [47]:

- le consentement
- la transparence
- le droit des personnes
- la responsabilité

Pour recueillir et utiliser les données personnelles, les entreprises doivent obtenir le **consentement** des personnes. Ce consentement doit être explicite et positif. Par conséquent, le fait de préremplir le formulaire d'acceptation des conditions générales avant validation n'est plus permis. Point important, ce consentement peut être retiré à tout moment [47]. Le responsable du traitement de ces données devra également être à même de prouver le consentement.

En matière de **transparence**, les entreprises doivent indiquer qui elles sont et dans quels buts elles vont traiter nos données [45]. Elles doivent également indiquer de manière claire, concise et compréhensible de quelles façons les données seront traitées [47].

En matière de droit des personnes, nous mentionnerons les 4 articles suivants :

- **le droit d'accès aux données (Article 15)**
  ce droit permet à toute personne de demander à une entreprise quelles sont les données dont elle dispose sur cette personne. Elle permet également de demander une copie de ces données. Cela permet par exemple de vérifier que les données sont correctes et à jour [46].
- **le droit de faire rectifier les données (Article 16)**
  Cet article donne le droit de modifier des données incorrectes ou de compléter des données jugées incomplètes [46].

- **le droit à l'effacement (Article 17)**
  L'entité qui traite nos données personnelles devra les effacer dans les meilleurs délais dans lorsqu'un des cas suivants est vérifié [46]:
  - *« nos données ne sont plus nécessaires au regard des finalités »*
  - *« nous retirons votre consentement sur lequel est fondé le traitement et il n'existe pas d'autre fondement juridique au traitement »*
  - *« nous nous opposons au traitement de vos données et il n'existe pas de motif légitime impérieux pour le traitement »*
  - *« nos données personnelles ont fait l'objet d'un traitement illicite »*
  - *« nos données personnelles doivent être effacées pour respecter une obligation légale »*

  Le **droit à l'oubli** est la suite du droit d'effacement. Lorsqu'une personne demande à une entreprise de supprimer des données personnelles et que ces données ont été rendues publiques, l'entreprise doit prendre des mesures raisonnables pour demander aux sociétés disposant d'une copie de ces données d'effacer à leur tour ces informations [46].

- **le droit à la portabilité des données (Article 20)**
  Le droit à la portabilité permet de récupérer nos données auprès d'une entreprise et de les transférer auprès d'une autre entité. Cela permettra de changer plus facilement de fournisseur de service [46].

Les nouvelles règles visent également à **responsabiliser** les entreprises quant au traitement de nos données. Ainsi, elles doivent notifier les autorités compétentes en cas de destruction, perte ou vol de données personnelles, et ce, dans les 72 h [47]. En outre, elles doivent documenter les procédures utilisées en vue de la protection des données et désigner un Délégué à la protection des données qui se charge du respect des différents points du RGPD [47].

En cas d'abus, tout le monde peut porter plainte gratuitement auprès de l'Autorité de protection des données (anciennement appelée commission de la vie privée). Dernier point important, le RGPD inverse la charge de la preuve. C'est désormais à l'entreprise de prouver sa bonne foi. [48]

Les violations du règlement pourront engendrer des amendes allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire mondial [45].

Il y a évidemment énormément de choses à dire au sujet de ce nouveau règlement. Nous avons présenté ici un bref aperçu, le but de ce travail n'ayant pas trait aux aspects légaux, mais au ressenti des personnes quant à l'utilisation de leurs données personnelles. Le lecteur intéressé pourra se référer au site internet de l'Autorité de protection des données (https://www.autoriteprotectiondonnees.be/ - [46]) pour des informations plus approfondies sur le sujet.

Chapitre 4 - Etude de marché

Ce chapitre décrit les résultats obtenus lors de notre étude de marché. La première section présente les objectifs et la méthodologie suivie pour cette étude. La seconde section contient la liste des questions posées lors de cette étude. La troisième partie rassemble objectif par objectif les réponses obtenues et les conclusions que nous pouvons en tirer.

4.1. Objectifs de l'étude et méthodologie utilisée

Dans le cadre de ce travail, nous avons effectué une étude de marché qualitative. Pour ce faire, nous avons suivi les lignes directrices décrites dans [49]. Cette étude consistait en différents entretiens individuels réalisés auprès d'un échantillon de 8 personnes dont les tranches d'âges et professions sont décrites dans le tableau ci-dessous.

Profession/domaine d'activités	Tranche d'âge
Etudiante en droit	20-25 ans
Assistante sociale	25-30 ans
Doctorant	25-30 ans
Traductrice	25-30 ans
Ressources humaines	30-35 ans
Informaticien	45-50 ans
Institutrice retraitée	60-65 ans
Ingénieur retraité	60-65 ans

Les questions ouvertes posées lors des entretiens (cf. section suivante) ont pour objectif de répondre aux questions suivantes :

1. Faire un état des lieux, comprendre la position des consommateurs par rapport aux données collectées à leur sujet ; en sont-ils conscients ? Y sont-ils favorables ? Y voient-ils un danger ?
2. Comprendre les freins par rapport au partage de données personnelles.
3. Comment les consommateurs réagissent-ils par rapport à une utilisation abusive de leurs données personnelles (ex. scandale Cambridge Analytica).
4. Quelle valeur associent-ils aux données qu'ils partagent au quotidien ? Qu'en attendent-ils en échange ? Estiment-ils que leurs données ont une valeur ?
   Sont-ils prêts à partager davantage d'informations pour obtenir des réductions et des offres personnalisées ?
5. Est-ce que les personnes interrogées ont confiance dans le traitement de leurs données personnelles ?
6. Quelle est la connaissance des personnes interrogées sur les règles de protection des données en vigueur actuellement ?

4.2. Liste de questions posées

Pour atteindre les objectifs évoqués ci-dessus, nous avons constitué la liste de questions suivantes. Chacune d'entre elles est associée à un des objectifs. Ce sont ces questions qui ont été posées lors des différents entretiens.

1. Etes-vous un utilisateur régulier de Google et/ou Facebook ? (Objectif #1 – état des lieux)
2. Quels sont les avantages que vous percevez par rapport à l'utilisation de ces services ? (ex : gain de temps, rester en contact avec ses amis/connaissances, se tenir informé par rapport à des évènements (activités, expositions, soirées, etc.)) (Objectif #1 – état des lieux)
3. Recevez-vous des notifications pour des promotions ou des suggestions d'articles que vous pourriez aimer sur base de vos recherches précédentes ? Qu'est-ce que cela vous inspire ? Est-ce positif ? Est-ce que cela vous inquiète ? (Objectif #1 – état des lieux)
4. Un centre commercial français a utilisé les données de géolocalisation des clients pour leur proposer des offres ciblées et des offres de réduction lors de leur passage dans les magasins. Qu'en pensez-vous ? Etes-vous favorable à ce genre de pratiques ? (Objectif #1 – état des lieux)
5. Est-ce que vous pensez que le consommateur est suffisamment protégé par les règles de Facebook et Google ? (Objectif#5 - confiance)
   Faites-vous confiance à Facebook et Google quant à l'utilisation de vos données ?
   Est-ce que vous estimez que ces données sont en sécurité ?
6. De manière générale, pensez-vous que les sociétés en font suffisamment pour la protection de nos données personnelles ? (Objectif#6 – connaissance des règles)
7. Facebook et Google sont deux entreprises très profitables (4 milliards de dollars de bénéfices pour Facebook en 2017 – 12.7 milliards pour Google en 2017), savez-vous d'où proviennent ces revenus ? (Objectif#4-valeur des données)
8. Pensez-vous que Facebook et Google vendent nos données à des tiers ? (Objectif#5 – confiance - Objectif#6 – connaissance des règles)
9. Utilisez-vous un pseudonyme ou donnez-vous de fausses informations lorsque vous remplissez un formulaire en ligne de manière à protéger votre vie privée ? (Objectif#5 - confiance)
10. Début 2018, des articles sont parus dans la presse au sujet d'un vol massif des données de 87 millions d'utilisateurs Facebook. Ces données ont été utilisées pour tenter d'influencer le vote lors de la dernière élection présidentielle américaine. Des soupçons d'activités similaires pèsent sur des manipulations de référendum du Brexit. Que pensez-vous de cette affaire ? (Objectif#3-réaction utilisation abusive des données)
11. Un nouveau règlement général sur la protection des données va entrer en vigueur en mai 2018 pour protéger le citoyen européen contre une utilisation abusive de ses données personnelles. En avez-vous entendu parler ? Qu'en pensez-vous ? (Objectif#6 – connaissance des règles)
12. Connaissez-vous les règles en vigueur en Belgique et en Europe sur la protection des données personnelles ?
    Si oui, pourriez-vous m'en citer une ou deux ?
    Si non, quelle serait pour vous une règle indispensable à implémenter ?
    (Objectif#6 – connaissance des règles)
13. Effectuez-vous des achats en ligne ?
    Lors de ces achats, êtes-vous prêts à partager des informations vous concernant pour obtenir des réductions et des offres personnalisées ? (Objectif#4-valeur des données)
14. Quel serait le type de données que vous ne souhaiteriez pas partager ?
    Celles que vous accepteriez de partager sans souci ? (Objectif#2-compréhension des freins)
15. Est-ce que le fait de pouvoir effacer/contrôler les données à votre sujet vous inciterait à partager davantage d'informations ? (Objectif#2-compréhension des freins)
16. Pensez-vous qu'il y a suffisamment de transparence de la part de Facebook et Google par rapport à la collecte de données ? Sinon, que souhaiteriez-vous changer ?
    (Objectif#2-compréhension des freins)

17. Avez-vous déjà pensé à l'impact que les données que vous partagez actuellement pourraient avoir à long terme ? (Objectif#2-compréhension des freins)
18. Courte vidéo (febelfin – www.safeinternetbanking.be) de sensibilisation aux dangers du net : https://www.youtube.com/watch?v=_kbVBOQ0J5w
    Qu'est-ce que cela vous inspire ? (Objectif#3-réaction utilisation abusive des données)
19. Une enquête de test achats a montré récemment la vulnérabilité de certains objets connectés : montre GPS, tablette pour enfant, serrure connectée. Qu'en pensez-vous? (Objectif#3-réaction utilisation abusive des données)
20. Seriez-vous prêt à payer pour utiliser les services de Google et Facebook et ainsi éviter la publicité ? (Objectif#4-valeur des données)
21. En matière d'assurance auto, seriez-vous prêt à équiper votre véhicule d'un boitier, mesurant la vitesse, position GPS, style de conduite, pour payer votre assurance au Km et bénéficier d'une réduction ? (Objectif#4-valeur des données)

4.3. Objectif #1 : Etat des lieux sur la position du consommateur par rapport à la collecte de données personnelles

Objectif #1: état des lieux, compréhension de la position des consommateurs par rapport aux données collectées à leur sujet ; en sont-ils conscients? Y sont-ils favorables? Y voient-ils un danger?
Questions #1 - #2 - #3 - #4

4.3.1. Utilisation de Google et Facebook

Sans surprise, toutes les personnes interrogées utilisent énormément Google et Facebook. Les réponses obtenues ci-dessous décrivent l'avantage perçu par les personnes interrogées quant à l'utilisation des services offerts par Google et Facebook.

« *Par rapport à Google l'avantage c'est que ça me permet de faire des recherches rapides il me faut une information, il faut calculer un trajet, il ne me faut une image pour une présentation, etc. c'est la rapidité de l'information tout est rassemblé sur une énorme base de données. Pour moi c'est l'avantage principal.* »

Google drive est également utile aux étudiants :

« *Pour ce qui est de Google, j'utilise la messagerie Gmail ainsi que Google drive. D'ailleurs on utilise Google Drive tout le temps pour les travaux de groupes pour partager les documents. Et ce qui est pratique aussi, c'est que nous pouvons éditer un document à plusieurs personnes en même temps.* »

Certaines personnes ont essayé des alternatives aux moteurs de recherche Google :

« *Google c'est mon moteur de recherche habituel, j'ai essayé des alternatives comme Yahoo et ça ne me plaît pas. Il y a Ecozia aussi, mais ils n'ont pas les mêmes référencements donc voilà je suis revenu à Google.* »

La réponse suivante résume bien les commentaires des différentes personnes de l'échantillon :

« *Google fournit beaucoup de services qui rendent notre vie plus facile comme Google Maps par exemple. Et chaque fois que je souhaite avoir une information sur Internet, je passe par Google. Ainsi par exemple, si je veux savoir ce que veut dire GDPR j'utilise Google. Dans notre vie courante, on ne peut pas vraiment vivre sans ces services. J'utilise également la messagerie Gmail, Google translate etc.* »

Pour ce qui est de Facebook :

« Facebook c'est plus pour garder le contact avec mes amis étant donné que j'habite à l'étranger depuis plusieurs années. Ca me permet de garder le contact avec les personnes que j'ai rencontrées lors de mes différents voyages. J'ai ainsi pu retrouver des amis d'enfance que je n'avais plus vus depuis de très nombreuses années. En fait, ça permet de rapprocher les distances. Grâce à ça je peux partager de bonnes nouvelles avec les autres, mais je mets certaines limites je ne partage pas toutes mes informations privées sur Facebook évidemment ».

Plusieurs personnes ont aussi mentionné le fait de pouvoir organiser des évènements facilement. Les étudiants utilisent également Facebook pour échanger des informations au sujet des cours, des examens, s'entraider sur certains sujets :

« *Pour Facebook, c'est plutôt un usage récréatif, mais c'est utile pour les cours aussi, pour partager les questions des examens des années précédentes par exemple.* »

Certaines personnes ont également cité Facebook comme moyen d'accès à l'information via les pages de différents journaux ou magazines. Plusieurs personnes ont indiqué voir parfois le temps passé sur cette plateforme comme une perte de temps.

« *Pour Facebook c'est plus une perte de temps, je l'utilise mais parfois j'arrête de l'utiliser pendant certaines périodes. D'un côté, cela permet de rester en contact avec ses amis ce qui est une bonne chose et de voir ce qu'ils deviennent mais d'un autre côté je me dis parfois que je n'ai pas vraiment besoin de connaître toutes ces informations. Par le passé, on perdait plus facilement le contact avec ses amis alors que maintenant grâce à Facebook, les choses sont différentes.* »

Beaucoup ont également mentionné « *Facebook Messenger* » comme un moyen de communication très utile pour discuter avec leurs amis.

4.3.2. Réactions par rapport à la publicité ciblée

Les personnes interrogées se rendent compte que leurs données personnelles sont utilisées à des fins de marketing.

« *Oui, je reçois beaucoup de publicités ciblées, par exemple quand on regarde pour réserver un hôtel via Google, on reçoit des offres publicitaires pendant une semaine. Souvent, ça reste quelques jours et après ça repart. En fait dès que l'on regarde n'importe quel article on reçoit des pubs par après. Et sur n'importe quel site. Par exemple, j'utilise un traducteur en ligne 'linguee' et là j'ai toujours des pubs associées à mes recherches précédentes.* »

Pour certaines personnes, ce ciblage publicitaire n'est pas dérangeant :

« *Ça ne me dérange pas vraiment car je suis conscient que ces sociétés connaissent ces informations à mon sujet. Ça renforce simplement le fait que les sociétés connaissent énormément de choses à mon sujet, mais je trouve quand même que c'est un peu étrange. Dans certaines circonstances c'est un peu inattendu par exemple quand je vais chez Tesco, on me propose des articles qu'un de mes anciens colocataires a achetés il y a plusieurs années.*

Également, sur Google je reçois des publicités pour des recherches que j'ai effectuées récemment. Mais je me dis voilà ils ont toutes ces informations à ce sujet et je comprends qu'ils souhaitent les utiliser. Personnellement je souhaiterais qu'ils ne les utilisent pas. En fait, je souhaiterais que ces sociétés ne disposent pas de toutes ces informations à mon sujet, mais je réalise que s'ils ne faisaient pas ça ils commenceraient à nous faire payer pour utiliser les services. Il y a du positif et du négatif dans chaque situation. »

Le fait que les données utilisées pour le ciblage ne sont pas jugées comme sensibles favorise l'acceptation du ciblage publicitaire :

« *Je ne m'inquiète pas beaucoup pour l'instant, car ce ne sont pas des données sensibles je reçois des promotions pour des chaussures, des vêtements, de la déco, du mobilier, etc. car c'est la plupart des trucs que je like sur Facebook. Il n'y a rien de bizarre par rapport aux suggestions.*»

Par contre si ces données utilisées étaient plus sensibles et concernaient des informations relatives à l'état de santé, la perception de la publicité ciblée serait différente :

« *Ce qui me choquerait c'est que si j'avais des problèmes de santé on me propose des produits en adéquation avec ça. Mais pour l'instant je ne ressens pas ce type de choses et si je reçois de la publicité qui ne m'intéresse pas je passe au-delà et je ne m'inquiète pas.* »

Toujours en lien avec la santé :

« *Lorsque j'étais enceinte, après quelques semaines j'ai commencé à recevoir des publicités pour des articles pour Bébé. C'était quand même très surprenant, d'autant que peu de personnes étaient au courant… je trouve que là ça va trop loin …* »

Certaines personnes trouvent la publicité utile, sur Amazon par exemple, le fait d'avoir des propositions pour des articles similaires est jugé utile. Plusieurs personnes ont également indiqué être peu sensibles à ces publicités:

« Je pense que ça n'influence pas plus que ça mon comportement, mais peut être que de manière indirecte si. »

La publicité ciblée serait également jugée comme dérangeante si elle occasionnait des pertes de temps.

D'autres personnes sont moins favorables à la publicité ciblée:

« C'est en quelque sorte une preuve d'espionnage. C'est même assez inquiétant. »

« Je pense que c'est fort embêtant de recevoir toutes ces publicités parfois on a limite peur d'effectuer une recherche sur un truc parce qu'on sait qu'on va être embêté pendant une semaine avec toutes les pubs. C'est quand même assez invasif. On se rend compte qu'on sait tout ce qu'on fait. »

Même si ces personnes sont dérangées ou inquiètes par rapport à ça, leur inquiétude reste modérée :

« *En plus, depuis peu de temps, le fait d'avoir des publicités qui pourraient te plaire sur Facebook, ça fait peur, mais ce n'est pas comme un film d'horreur.* »

4.3.3. Réactions par rapport au ciblage publicitaire dans un supermarché

Aucune des personnes n'a indiqué être intéressée par un ciblage publicitaire lors de son parcours d'achat dans un centre commercial (cf. question #4).

« *Pour ce qui est du magasin, je ne pense pas que ce soit particulièrement une bonne idée. Je ne souhaite pas recevoir de la publicité ciblée en fonction de la position dans un centre commercial. Mais d'un autre côté si les clients souhaitent recevoir ce service et recevoir des offres qu'ils ne recevraient pas autrement. C'est ok d'offrir ce type de service.* »

En outre, plusieurs répondants ont indiqué l'importance d'informer les clients avant de leur fournir ce type de service :

« Pour moi le plus important c'est que les gens qui bénéficient de ce service savent qu'ils sont suivis dans les magasins et que le magasin leur donne le choix d'utiliser ce service. Utiliser directement ces données sans que les gens sachent, je ne suis pas d'accord avec cette approche, car on ne donne pas toute l'information aux personnes et je suis pour un échange ouvert d'informations. »

De nombreuses personnes ont également mis en avant le côté envahissant de ce type de système

« *C'est quand même fort envahissant. À chaque fois on croit qu'on a reçu un message alors que ce sont simplement les notifications du magasin. Ça détourne l'attention. Et puis, ça peut être aussi de la mauvaise publicité : on ne va peut-être plus aller là, car nous avons reçu plein de notifications et c'est pénible. Ça va peut-être aussi détourner des clients de ce centre commercial là. En tout cas, si je commençais à recevoir beaucoup de notifications, je ne resterais pas longtemps dans ce magasin, je pense que je partirais.* »

Certains reçoivent déjà ce type de notification en fonction de leur géolocalisation :

« *Moi j'ai le cas avec Nespresso. J'ai téléchargé l'application qui me permet de commander mes capsules de café et de me les faire livrer directement au bureau ce qui est un gain de temps pour moi. Mais cette application utilise la géolocalisation de mon téléphone et dès que je m'approche d'une boutique Nespresso elle m'envoie une notification sur mon smartphone.*

Ça je trouve assez flippant, car les gens savent où je suis… Bon, dans ce cas-ci c'est Nespresso je ne m'inquiète pas, mais quelqu'un qui malintentionnés quelqu'un qui a de bonnes compétences en IT pourrait savoir où je suis. Ça c'est le genre de truc qui me rend un peu plus parano. »

Ces mêmes personnes reconnaissent l'intérêt de la géolocalisation dans certains cas:

« Par contre, la géolocalisation de mon smartphone a aussi des avantages. Par exemple, quand je souhaite dire à des amis ou à mon copain je peux partager ma géolocalisation avec eux via WhatsApp»

4.3.4. En résumé

Objectif #1 : Faire un état des lieux, comprendre la position des consommateurs par rapport aux données collectées à leur sujet ; en sont-ils conscients ? Y sont-ils favorables ? Y voient-ils un danger?

Les personnes interrogées sont conscientes que leurs données personnelles sont utilisées à des fins de marketing direct. Ces utilisations sont jugées comme peu dérangeantes pour autant qu'elles n'occasionnent pas de pertes de temps et concernent des informations jugées peu sensibles (mobilier, décoration, achats alimentaires, etc.). Le fait que les gens puissent faire le lien entre les publicités qui leur sont soumises et les informations sur lesquelles ces pubs sont basées semble réduire les inquiétudes.

La limite évoquée par plusieurs personnes concerne les informations relatives à la santé. L'utilisation de ces informations très personnelles est mal perçue.

Les personnes moins favorables à la publicité ciblée se disent inquiètes, mais pas au point de ne plus utiliser les services en ligne. Toutes les personnes interrogées sont conscientes que l'utilisation de leurs données personnelles est en quelque sorte la contrepartie d'un service gratuit.
Pour ce qui est de la publicité ciblée sur base de la géolocalisation dans les centres commerciaux, aucune des personnes interrogées n'était intéressée par ce service. Toutes ont mis en avant l'importance d'avertir le consommateur au préalable et certaines personnes ont mis en avant le côté envahissant de ce type de notifications voir la mauvaise publicité pour le centre commercial si ce type de système était mis en place.

4.4. Objectif #2 : Compréhension des freins par rapport aux partages de données personnelles.

Objectif #2 : Compréhension des freins par rapport aux partages de données personnelles.
Questions #14 – #15 – #16 – #17

4.4.1. Sensibilité du type de données

Par rapport aux types d'informations qui peuvent être partagées et celles qui sont considérées comme étant plus privées (question #14), nous avons obtenu plusieurs réponses unanimes. Les répondants sont prêts à partager sans souci des données telles que l'âge, sexe, taille, nom, prénom,…

De même, les informations bancaires et médicales sont considérées comme étant privées. Il en va de même pour les conversations privées par l'intermédiaire de messageries telles que « *Facebook-Messenger* » et l'historique de recherches sur internet :

« Est-ce que tu trouves que ton historique de recherche sur Internet est sensible? Là aussi c'est une question intéressante, car quand je fais cette recherche sur Internet je me rends compte que certains thèmes ne sont pas forcément bien perçus par l'opinion générale. En tout cas pas autant que je souhaiterais qu'ils le soient. Donc dans ce cas-là je fais des recherches avec un navigateur en mode privé. Donc forcément je n'aimerais pas partager ces idées-là. Je me sentirais jugé par une société n'est pas suffisamment ouverte. En tout cas, qui juge directement avant de voir les choses dans leur contexte. »

Pour d'autres informations comme le comportement d'achat, les réponses diffèrent en fonction des personnes interrogées :

« Des données marketing sur des comportements d'achats, ça j'estime que ce n'est pas très important. »

Alors que pour d'autres :

« Donc c'est quelque chose que je ne préfère pas partager, car certaines personnes ne sont pas capables d'avoir une opinion nuancée et pourraient directement me juger. »

Chose étonnante, le numéro de téléphone est vu par beaucoup de personnes comme étant une information qu'ils ne souhaitent pas partager alors qu'il y a quelques années encore, ces informations figuraient pour une part importante de la population dans des bottins de téléphone.

4.4.2. Contrôle des données et droit à l'oubli

Le fait de pouvoir effacer/contrôler les données partagées avec certaines entreprises ou certaines plateformes n'inciterait pas beaucoup de personnes à partager davantage d'informations (Question #15)

« Non pas du tout. Car c'est internet et on sait très bien qu'une fois que nos informations sont sur internet elles sont sur internet à vie. Il vaut mieux ne pas partager du tout que de partager et ensuite essayer de corriger le tir. »

« Non, ça ne m'inciterait pas à partager davantage d'informations, car si je partage des informations dès le départ, c'est que j'ai un niveau de confiance suffisant dans l'entreprise. »

Plusieurs répondants ont également fait état d'un manque de confiance quant à la suppression effective de ces données :

« Non j'aurais peur que ces données ne soient pas effectivement effacées. Non je n'aurais pas confiance par rapport à ça car je n'aurais pas de moyen de contrôler ça. »

Seule une personne a répondu favorablement à la question #15 :

« oui ça m'inciterait à partager plus d'informations mêmes si je ne les supprimerais peut-être jamais, mais oui ça m'inciterait. Par exemple sur Facebook. J'avais partagé un poste de Donald Trump sur Twitter et par la suite en y réfléchissant j'ai retiré mon poste Facebook, car ce message sorti de son contexte aurait pu donner une mauvaise image de moi. Je pense que je n'aurais jamais posté ce message sur Facebook si j'avais su que je ne pourrais pas le supprimer par la suite. »

Par contre, l'avis était unanime par rapport au droit à l'oubli implémenté dans le nouveau règlement européen GPDR.

« Par contre, le fait de pouvoir demander à chaque entreprise de pouvoir effacer les informations dont elle dispose à notre sujet est un des grands avantages du nouveau règlement européen. »

4.4.3. Transparence quant à l'utilisation des données personnelles

Seule une personne estime qu'il y a suffisamment de transparence de la part de Google et Facebook quant à l'utilisation de ses données personnelles :

« Je pense qu'ils essayent d'être transparents, mais je ne prends pas suffisamment de temps pour lire leurs règles d'utilisation donc je dirais a priori oui. Je ne vois pas comment on pourrait encore améliorer la chose pour l'instant, car ils envoient un grand nombre de messages pour expliquer ce qu'ils font. Je les ai lus en diagonale et je pense que ça m'avait l'air correct.

Je n'ai pas suffisamment lu dans les détails, mais les éléments que j'ai lus, me semblaient suffisamment clairs. J'ai essentiellement recherché certains mots-clés dans le texte, mais de nouveau comme je pense ne rien avoir à cacher je n'ai pas poussé l'analyse au maximum. »

D'autres ressentent un manque de transparence:

« Non, probablement pas. C'est une entreprise qui dispose de milliards d'utilisateurs et qui emploie plusieurs centaines de personnes, c'est donc difficile pour eux d'être totalement transparents. De plus, serai-je en mesure de comprendre tout ce qu'ils font ?

De plus, est-ce qu'une société a vraiment envie d'être transparente par rapport à tout ce qu'elle fait. Ces sociétés veulent également gagner de l'argent. Peuvent-elles être davantage transparentes ? Probablement, mais à quel point, je ne sais pas. Je pense qu'ils sont relativement transparents. »

D'autres soulignent le manque de clarté des conditions d'utilisations :

« Non, on sait qu'ils utilisent nos données, mais on ne sait pas trop pourquoi. Et quand l'information est communiquée dans les conditions générales, ce n'est pas suffisamment clair … C'est la différence entre « est-ce que les informations sont accessibles » et « est-ce qu'elles sont utilisées ». Je pense que ces infos sont accessibles quelque part, mais après est-ce que c'est suffisamment accessible pour que le consommateur les lise et en prenne connaissance. Ils devraient davantage travailler là-dessus. Mais je pense que c'est un peu une volonté de leur part. Ils les cachent un petit peu comme ça personne ne va les lire et ils auront satisfait leurs obligations légales. Ils ont communiqué, mais en pratique personne n'est au courant, car personne ne va lire ces informations. »

4.4.4. Conséquences à long terme

La plupart des personnes interrogées a conscience que l'information partagée peut avoir des conséquences à long terme. C'est par exemple le cas des photos postées sur Facebook. Celles-ci sont choisies pour ne pas donner une mauvaise image de soi dans le milieu professionnel par exemple. Certains se sont posés la question, mais ne voient pas d'inconvénients par rapport aux informations qu'ils partagent à l'heure actuelle.

D'autres évoquent des inquiétudes par rapport aux données médicales ou certaines dérives :

« Conserver une grande quantité d'informations pourrait avoir des implications importantes dans le futur. Pour la plupart de ces données, cela n'a pas beaucoup d'importance, par exemple ma marque de café préférée, mais il y a également certaines données que je ne souhaite pas voir diffuser.

Je ne souhaiterais pas que ma compagnie d'assurance ait accès à mon dossier médical par exemple. De plus, si quelqu'un avait un échantillon de mon ADN il pourrait estimer mon espérance de vie, ou encore le nombre de chances que ma fille a de développer telle ou telle maladie dans le futur. Donc ça pourrait avoir un impact pour moi, mais aussi pour ma famille.

En outre, il y a beaucoup de cas dans le monde où des policiers ont par exemple utilisé les outils mis à leur disposition pour obtenir des informations sur leur conjoint ou ex-conjoint. Je ne pense pas que les gouvernements démocratiques pourraient en faire un mauvais usage, mais si ces données étaient piratées certaines personnes pourraient en faire un mauvais usage et cela pourrait avoir des conséquences importantes. »

4.4.5. En résumé

Objectif #2 : Comprendre les freins par rapport aux partages de données personnelles.

Les informations que les répondants acceptent de partager sans souci concernent l'âge, le sexe, la taille, le poids, ainsi que les noms et prénoms. A l'inverse les données bancaires et médicales sont considérées comme étant très privées par l'ensemble des personnes interrogées. Des données telles que le comportement d'achat sont parfois considérées comme étant sensibles par certains alors que d'autres personnes ne voient pas d'objection à les partager. Les informations de géolocalisation sont également jugées comme étant privées même si le partage de la position GPS est utile dans certains cas pour retrouver ses amis lors d'un évènement par exemple. Etonnamment, le numéro de GSM est considéré par certains comme une donnée privée qu'ils évitent de partager sur les réseaux sociaux ou simplement par message.

Nous ressentons un manque de confiance par rapport à l'utilisation des données personnelles. Le droit à l'oubli est vu comme un aspect très positif du nouveau règlement européen, mais beaucoup s'interrogent quant à la suppression effective de ces données : les données seront-elles effacées, qui effectuera le contrôle, etc. En tout cas, cette mesure n'incitera pas les utilisateurs à partager davantage d'informations personnelles.

La majorité des personnes interrogées ressentent un manque de transparence quant au traitement de leurs données. Beaucoup de personnes ont indiqué que des conditions générales d'utilisation plus claires et plus lisibles les rassureraient sur ce point.

4.5. Objectif #3 : Réactions par rapport à une utilisation abusive des données personnelles

Objectif#3 : Comment les consommateurs réagissent-ils par rapport à une utilisation abusive de leurs données personnelles (ex : scandale Cambridge Analytica)
Questions #10 – #18 – #19

4.5.1. Réactions suite à la diffusion de fausses informations en vue d'influencer des élections

La question #10 relative au vol de données de millions d'utilisateurs Facebook en vue d'influencer des élections n'a pas surpris les personnes interrogées. Beaucoup estiment en effet que ce canal peut être un moyen efficace pour tenter d'influencer l'opinion.

« Je pense que c'est possible d'influencer l'opinion avec des fausses infos via les réseaux sociaux en publiant des messages à l'aide de faux comptes comme l'a fait la Russie. Ces fausses informations ont été vues par énormément de personnes et je pense que pas mal de ces personnes ont pu être influencées par cela. Beaucoup utilisent Facebook pour s'informer. Donc pour influencer les gens c'est peut-être un des moyens les plus efficaces. »

Beaucoup ont souligné la difficulté de discerner les informations véridiques des informations erronées ou mal intentionnées sur internet :

« Je trouve qu'il y a beaucoup de 'fake news' sur Facebook. Ce n'est pas évident de distinguer la vraie info de la fausse info. C'est donc facile de faire passer de fausses infos par cet intermédiaire. »

« Je trouve que le problème sur Internet c'est que l'on peut faire croire à peu près tout et n'importe quoi à des personnes qui ne sont pas très critiques par rapport à l'information qu'elles reçoivent. Par exemple, je m'intéresse beaucoup à la nutrition et c'est très difficile de trouver des informations qui ne sont pas erronées. »

« Avant quand tu avais besoin de certaines informations, tu devais aller à la bibliothèque. Maintenant, il suffit de quelques clics et tu as toutes ces informations-là très rapidement. Mais l'inconvénient c'est qu'il y a moins de contrôle de l'information. N'importe qui peut écrire sur n'importe quel sujet et le faire passer pour un document véridique et scientifique ce qui peut induire des gens en erreur et ainsi les manipuler. Je pense par exemple à une histoire récente au sujet de vaccins. Des gens déclarent sur des réseaux sociaux que les vaccins nuisent à la santé et sont juste des inventions des compagnies pharmaceutiques pour gagner de l'argent. Alors qu'en réalité ces articles se basent sur des informations qui ne sont pas fondées et sont rédigées par des personnes qui ont peu de connaissances scientifiques. Cela a comme conséquence qu'une partie de la population croit aujourd'hui que les vaccins sont produits par des compagnies pharmaceutiques uniquement pour faire de l'argent et que ces vaccins tuent des enfants.

Plusieurs personnes interrogées ont également mentionné que même si le vol de données les choque, c'est surtout le manque d'esprit critique des internautes qui est remis en cause :

« Le problème c'est que les gens manquent d'esprit critique et ne prennent pas de recul par rapport aux informations. L'immigration est également un sujet fort sensible et les réseaux comme Facebook permettent à tout le monde et n'importe qui de partager ce qu'ils pensent à ce sujet avec des situations qui s'enveniment. Je pense qu'aujourd'hui cela peut faire partie d'un nouveau système de propagande si les réseaux sociaux ne sont pas utilisés correctement. »

« J'estime que c'est aussi à la personne qui reçoit des informations sur Internet de faire la part des choses et ne pas se laisser berner par les informations qu'elle reçoit. Je pense aussi que ce serait intéressant qu'il y ait un organisme qui s'occupe de ces messages erronés et de ces fausses informations qui circulent sur Internet. En pratique c'est un problème très complexe et je ne vois pas comment le résoudre facilement.

Ce type de dérive pourrait amener certaines personnes au pouvoir, je veux dire que le comportement qui pose le plus problème n'est pas le vol de données, mais la mauvaise utilisation qui en est faite et les fausses informations qui sont véhiculées. »

Enfin, le vol de données personnelles inquiète certaines personnes, mais pour elles les données sensibles ne se trouvent pas sur Facebook, mais ont plutôt attrait à la santé :

« Cela va de toute façon arriver en raison de la quantité d'informations que l'on partage sur ces plateformes. Je suis plus inquiet par rapport aux informations collectées par le gouvernement. Par exemple, en Inde le gouvernement a décidé de constituer une grande base de données contenant l'ADN des citoyens. Pour constituer cette base de données, ils disent aux citoyens qu'ils ne peuvent pas bénéficier des revenus de l'État tant qu'ils n'ont pas donné un échantillon. À ce jour ils ont constitué une base de données de plus de 1 milliard de personnes. Et on sait très bien que partout où il y a des données en ligne ces données peuvent être piratées. Je pense qu'il y a beaucoup plus d'endroits inquiétants que Google et Facebook pour stocker ces données. »

Quand nous leur demandons si leur comportement en ligne a changé depuis l'affaire « Cambridge Analytica », personne n'indique avoir changé son comportement en ligne. Probablement parce que les répondants avaient déjà conscience des risques associés aux partages d'informations personnelles.

4.5.2. Réactions suite aux failles de sécurité observées sur les objets connectés

La majorité des personnes interrogées a conscience des risques associés aux objets connectés et n'est pas surprise, par rapport aux résultats de l'étude de tests achats. Seules les personnes plus âgées ont été surprises par cette étude:

« Je ne suis pas surpris, j'entendais d'ailleurs l'autre jour une histoire au sujet d'un baby phone contrôlé à distance ; les parents étaient surpris de voir quelqu'un discuter avec leurs enfants au travers de ce moniteur.

N'importe quel objet connecté peut être piraté, peu importe le niveau de sécurité et de protection. En effet, si des pirates peuvent rentrer dans le système de la NSA, du FBI, ou du gouvernement américain pour leur voler des morceaux de code alors que ces différentes organisations dépensent des millions en matière de sécurité informatique et bien les objets connectés dont on dispose dans nos maisons ne sont pas en sécurité.

Je pense que ces objets pourraient être codés de manière plus sûre mais au final ça ne ferait pas grande différence. C'est le gros problème avec ses objets qui sont produits en masse et à faible coût. On peut par exemple prendre le cas d'une bouilloire connectée reliée au smartphone et quand le réveil sonne le matin la bouilloire se met en route. Les gens ne vont pas mettre 100 € de plus pour avoir un objet bien sécurisé.

Cela pourrait aussi arriver avec des voitures connectées. Quelqu'un pourrait en prendre le contrôle lorsque vous conduisez et la faire freiner par exemple.

Le fait qu'Angela Merkel ait vu ses conversations privées écoutées par le gouvernement américain sans s'en rendre compte malgré la quantité d'argent dépensé par l'Allemagne pour protéger ses installations montre que tout est possible.

Mais c'est le monde dans lequel on vit, personne n'est prêt à se passer de son téléphone pour éviter les risques. »

Pour certains cette étude engendre beaucoup de craintes :

« Cette étude me fait peur. D'ailleurs, j'ai un ami qui a installé cette serrure connectée. Il me dit que c'est pour les courses. Avec son téléphone il ouvre la porte et comme ça quand il arrive avec les courses, la porte est déjà ouverte. Mais si ce n'est pas lui qui est derrière le téléphone ?

C'est comme avec mon ex-copain, il n'avait plus besoin de mettre son code avant de faire un versement avec son smartphone. Imagine que quelqu'un lui vole son téléphone ?

Ce sont toutes des choses comme ça qui par fainéantise nous rendent vulnérables.

C'est comme la voiture qui conduit toute seule : tu lui dis au travail et elle te conduit au travail. Mais imagine qu'un jour elle ne te conduise pas au travail… »

D'autres ne se sentent pas concernés:

« Non, je ne suis pas très nouvelles technologies, ce n'est pas dans ce domaine-là que je dépenserai de l'argent. Donc je ne me sens pas très concerné par cette problématique. En effet, j'ai un smartphone mais je ne l'utilise pas au maximum de ses possibilités et je n'envisage pas d'acheter des objets connectés. »

Pour la majorité des personnes interrogées, le risque est minime quant aux données contenues dans les objets connectés. Elles sont donc prêtes à courir le risque :

« J'ai conscience des dangers liés à ces objets connectés, mais on ne sait pas vraiment y échapper. »

« Avec le GSM il y a une caméra, mais lorsque j'utilise mon téléphone je l'oriente de telle manière à ce que la caméra ne me fixe pas et donc j'estime que le risque est nul. »

« La caméra sur le GSM par exemple je n'y pense pas, je pourrais très bien me faire espionner par quelqu'un par cet intermédiaire-là. »

Pour beaucoup la responsabilité du fabricant des objets connectés piratés est engagée :

« Je trouve que c'est inquiétant. Les fabricants devraient travailler sur la sécurité des objets avant de les mettre sur le marché. Ce n'est quand même pas normal qu'ils se rendent compte de ça après. Ils devraient faire un test avant la commercialisation. De plus, ce ne sont même pas les producteurs qui ont mis le doigt sur le problème, c'est test achats qui l'a découvert en faisant le test. »

Paradoxalement, ces personnes ne seraient pas prêtes à payer un supplément pour disposer d'une meilleure protection.

« Non, ce n'est pas dans ce domaine-là que je dépenserai de l'argent. »

Même si la majorité des personnes interrogées est au courant des risques associés à l'utilisation d'internet et des objets connectés, beaucoup ont souligné l'importance de sensibiliser davantage de monde aux dangers du net.

4.5.3. En résumé

Objectif #3 : Comment les consommateurs réagissent-ils par rapport à une utilisation abusive de leurs données personnelles (ex : scandale Cambridge Analytica).

Les personnes interrogées se disent conscientes des risques de vols de données personnelles et de la mauvaise utilisation qui peut en être faite. Les répondants ont mis en évidence l'importance de garder un esprit critique par rapport aux informations véhiculées sur internet, de prendre du recul et de recouper l'information.

Ce n'est pas nécessairement le vol de données partagées avec Facebook qui inquiète tant les membres du panel mais plutôt des informations plus privées relatives à la santé par exemple.

L'étude de test achat n'a pas surpris beaucoup de personnes interrogées. La plupart étaient déjà conscientes des risques encourus avec ces objets. Beaucoup de répondants ont immédiatement pensé à la caméra de leur smartphone en entendant les résultats de cette étude. Certains estiment que les risques sont minimes, car ils orientent leur téléphone de manière à ce que la caméra ne les fixe pas. D'autres n'y pensent pas trop et préfèrent vivre avec ce risque : pour eux, le fait de se passer de leur smartphone serait trop pénalisant.

Plusieurs personnes ont mis en cause la responsabilité du fabricant quant à la sécurisation de ces objets, elles estiment que ces entreprises devraient tester davantage leurs systèmes avant de commercialiser leur produit. Le fait que ces failles aient été découvertes par test achat et non pas par le fabricant lui-même en a choqué plus d'un.

Beaucoup ont indiqué l'importance de sensibiliser les consommateurs aux risques potentiels associés à ces objets et voient ce type d'études comme étant une très bonne chose.

4.6.Objectif #4 : Valeur associée aux données personnelles

Objectif #4: Quelle valeur associent-ils aux données qu'ils partagent au quotidien ? Qu'en attendent-ils en échange ? Estiment-ils que leurs données ont une valeur ?
Sont-ils prêts à partager davantage d'informations pour obtenir des réductions et des offres personnalisées ?
Questions #7 - #13 - #20 - #21

4.6.1. Sources de revenus de Google et Facebook

Quand nous avons demandé au panel d'où provenaient les sources de revenus de Google et Facebook (question #7), la majorité a indiqué la publicité et la vente d'informations. Seules deux personnes plus âgées ont indiqué ne pas savoir. Ces personnes n'ont pas de compte Facebook et utilisent Google de façon minimale pour effectuer quelques recherches et des envois d'e-mails via la messagerie Gmail.

« Il doit déjà y avoir une grosse partie issue de la vente d'informations à des organismes qui peuvent les utiliser. Je pense que la majorité doit venir de là car il ne faut pas payer pour s'inscrire. Tout l' argent qu'ils ont, je pense que ça vient de la pub et de la vente d'informations. Je pense qu'il y a une grosse partie issue de la publicité. Par exemple Google, tu payes pour être le premier en référencement. Sur Google, en général, les trois ou quatre premiers référencements ça dit 'annonce'.

Et sur Facebook ça doit être de la publicité, il y en a de plus en plus. Avant, c'était juste à droite. Maintenant c'est partout même dans Messenger. Après, tant mieux pour eux. Facebook, c'est un petit gars qui a décidé de faire une sorte de MSN et maintenant il y a plusieurs milliards d'utilisateurs. C'est bien pour eux. »

4.6.2. Achats en ligne et partage d'informations

Plusieurs personnes interrogées font certains achats en ligne. C'est surtout la facilité et le gain de temps qui sont mis en avant :

« Oui je fais pas mal d'achats en ligne. Je fais des achats en ligne car je trouve que c'est facile. Je prends par exemple le cas de mes capsules Nespresso, je les commande en ligne car on me les livre en 24h au travail. C'est surtout un gain de temps pour moi. »

Certaines personnes ne souhaiteraient pas partager davantage d'informations personnelles (question #13)

« Non je ne serais pas prêt à partager davantage d'informations pour obtenir des réductions. »

La raison mise en avant est la perte de temps occasionnée

« Non de nouveau la promotion sera sûrement de 5 % de 10 % et ça ne va pas m'intéresser. L'avantage offert doit être suffisant pour compenser le temps passé à remplir ce type de questionnaire. »

D'autres ne seraient pas contre pour autant que la perte de temps qui en résulte ne soit pas trop importante :

« Je ne sais pas trop, si ça ne prend pas beaucoup de temps et que la réduction en vaut la peine … il faut voir le rapport coût-bénéfice … si ça en vaut la peine pourquoi pas. »

Pour d'autres, cela dépend du type de questions posées, de plus il est important que ce type de questionnaire soit optionnel :

« Oui peut-être. De toute façon, je peux arrêter l'enquête à tout moment. Si un supermarché veut savoir quelle est ma marque de thé ou de café préférée, ça ne me dérange pas. Par contre, je ne vais pas leur donner des informations relatives à ma santé. Donc si ce type d'enquête est optionnel, oui peut-être. »

A noter que certains répondants ne font pas du tout d'achats en ligne pour éviter de partager des informations personnelles :

« Non je ne fais jamais d'achats en ligne, j'ai horreur de ça. Quand je dois faire des achats sur Amazon, je demande à quelqu'un de le faire pour moi (rire). Enfin si, parfois les billets d'avion. Et à chaque fois je suis fort stressée. Je ne comprends pas les gens qui achètent tout par Internet parce que c'est plus simple. Moi ça me fait peur, car ils ont toutes tes informations personnelles. En plus, avec ta carte de crédit ils vont se servir directement sur ton compte en banque.

Je n'ai jamais acheté sur Amazon, car je n'ai pas confiance tu ne sais jamais ce qu'ils font avec tes informations : ton adresse postale, ton adresse e-mail, etc. c'est le résumé de toi au final. Parce qu'en plus si tu achètes ils ont aussi ton numéro de carte de banque. En gros, ils toutes les informations qui figurent sur la carte d'identité ou quasi. Pour acheter un billet d'avion, tu dois mettre ton nom complet, ton numéro de passeport…

Donner toutes tes informations personnelles pour des vêtements par exemple, je trouve que ça n'en vaut pas la peine. C'est un risque et je n'aime pas même si je sais que de nos jours tout ça est très sécurisé. Donc si je peux éviter je le fais. »

4.6.3. Payer pour utiliser Google et Facebook

Seul un membre du panel serait prêt à payer pour bénéficier des services offerts par Google et Facebook (Question #20) mais pour autant que ce montant ne dépasse pas quelques euros par mois. Les autres se tourneraient vers des alternatives gratuites y compris les personnes les plus farouchement opposées à la collecte de données :

« Non. S'il faut payer, je n'utiliserai plus Facebook. Ce n'est pas vraiment nécessaire. Bon ça m'ennuierait car comme je te dis, ça me permet de rester en contact avec pas mal de monde.

Google ce serait un peu compliqué, mais bon, il y a pas mal d'alternatives même si ça va moins bien. Donc à ce niveau-là il n'y aura pas de souci. »

« Ça dépend combien … A priori … Enfin non … tant qu'il y a des alternatives gratuites je ne pense pas que je serais prête à payer pour utiliser ça. Pour Google il y a suffisamment d'autres messageries gratuites sur le marché pour ne pas avoir à payer. Les gens râlent quand on leur dit qu'on utilise leurs données mais si tu leur dit qu'ils doivent payer pour éviter ça, je pense que peu de monde serait prêt à payer pour utiliser Facebook. Je pense que le partage des données est la contrepartie du fait que l'inscription et l'utilisation soient gratuites. Pour eux tes données ont de la valeur, mais toi tu ne sais quand même pas en faire grand-chose, tu ne vas pas savoir vendre tes données… »

4.6.4. Partage de données et assurance

La majorité des personnes interrogées ne serait pas prête à partager des informations sur le style de conduite ou le kilométrage effectué pour bénéficier d'une remise sur la prime d'assurance. Plusieurs facteurs ont été mis en avant. Tout d'abord le montant de la réduction :

« Si c'est une toute petite réduction non mais si c'est une grosse réduction oui. Si c'était 25-30% c'est quelque chose que je serais prête à envisager, mais si ça augmente par la suite ce n'est pas vraiment intéressant … »

Pour d'autres, cela dépend du type de données partagées et de la confiance faite à l'organisme assureur :

« Ca dépend plutôt du type d'informations qu'ils collectent. Si c'est uniquement le style de conduite et la vitesse, ça ne m'inquiète pas, mais je ne veux pas qu'ils sachent où je vais. Cela dépend beaucoup des informations collectées du fait que je leur fais confiance ou pas. »

Les autres y sont opposés, car ils ne souhaitent pas partager leurs habitudes de vie ou pensent qu'un excès de vitesse les pénalisera fortement et annulera largement le bénéfice espéré grâce au partage d'informations.

4.6.5. En résumé

Objectif #4: Quelle valeur associent-ils aux données qu'ils partagent au quotidien ? Qu'en attendent-ils en échange ? Estiment-ils que leurs données ont une valeur ?
Sont-ils prêts à partager davantage d'informations pour obtenir des réductions et des offres personnalisées ?

La majorité des personnes interrogées est consciente du fait que la publicité est la source de revenus de Google et Facebook et que le partage de données personnelles est la contrepartie pour bénéficier de ces services « gratuitement ».

Certaines personnes seraient prêtes à partager davantage d'informations lors de leurs achats en ligne pour autant que

- cela n'occasionne pas de perte de temps ;
- ces questionnaires soient optionnels ;
- les questions posées ne soient pas jugées comme étant trop privées, des questions liées à leurs achats sembleraient acceptables.

Notons également qu'une personne interrogée indique ne pas faire d'achats en ligne pour éviter de partager ses informations personnelles. Pour elle, la quantité d'informations demandée est trop importante par rapport au gain de temps ou à l'aspect pratique des achats en ligne.

Seul un membre du panel accepterait de payer pour utiliser Google et Facebook pour autant que le montant ne dépasse pas quelques euros. Les autres préfèreraient se tourner vers des alternatives gratuites même si celles-ci sont moins performantes. Ce sentiment est partagé y compris par les personnes les plus farouchement opposées au partage de données.
En matière d'assurance, peu de répondants accepteraient de partager des informations liées à leurs trajets et leur style de conduite pour bénéficier d'une réduction. Le manque de confiance dans les organismes assureurs, le fait de devoir partager sa position géographique à tout moment et le risque de perdre davantage que le gain sur la prime en cas d'excès de vitesse sont autant de facteurs qui réduisent l'attrait de cette mesure. D'ailleurs, une réduction de 25%-30% du montant de la prime est évoquée avant d'envisager l'utilisation de ce système.

4.7.Objectif #5 : Confiance dans le traitement des données personnelles

Objectif #5: Est-ce que les personnes interrogées ont confiance dans le traitement de leurs données personnelles ?
Questions #5 - #6 - #8 - #9

4.7.1. Protection des données par les règles de Google et Facebook

La majorité des personnes interrogées estime ne pas être suffisamment protégée par les règles de Facebook et Google (cf. question #5.1)

« Je ne sais pas trop en fait. Je pense que maintenant ils sont tenus de le faire par le nouveau règlement européen, mais je ne sais pas jusqu'à quel point on est vraiment protégé. Le problème aujourd'hui avec les smartphones c'est qu'on ne contrôle plus vraiment l'intégrité de nos données. Avant on était beaucoup moins connecté qu'aujourd'hui et la maîtrise de l'information était beaucoup plus simple. Je trouve qu'on n'est pas vraiment protégé. »

Un autre indique que :

« Non, je pense d'ailleurs que c'est une des raisons pour lesquelles il y a le GDPR pour essayer de protéger les consommateurs. Même si je pense que les grosses multinationales essayent de se comporter de manière raisonnable avec les données collectées elles restent néanmoins des entreprises privées avec des actionnaires …

Je pense que nous avons besoin d'un contrôle du gouvernement sur les activités des sociétés par rapport à ce type de sujet. Non je ne pense pas que Google et Facebook en font suffisamment pour la protection de nos données, mais est-ce leur travail de faire ça- ? Je pense que c'est plutôt la responsabilité des gouvernements.

Je ne pense pas qu'ils en font suffisamment, mais je peux comprendre qu'ils n'en fassent pas davantage : ils pourraient se tirer une balle dans le pied en n'offrant pas un service que d'autres compagnies pourraient offrir à leurs clients et ainsi perdre un avantage. »

Quant à savoir s'ils font confiance à Facebook et Google quant à l'utilisation des données (cf. question #5.2), là aussi, la réponse est négative pour beaucoup de personnes interrogées :

« Non pas trop, mais je n'ai pas trop le choix si j'ai envie de poster certains messages et de les partager avec mes amis il faut bien passer par Facebook. Mais je fais attention si je partage quelque chose sur Facebook, car je sais que cette information va être partagée dans tous les sens donc je veille à ne pas partager des informations sensibles. »

« Non, les récentes affaires comme Cambridge Analytica ont montré qu'on ne pouvait pas leur faire confiance. Facebook a-t-il enfreint la loi dans cette affaire? Non, Cambridge Analytica a enfreint la loi. Mais dans le cadre de cette affaire, Facebook a reçu des informations concernant le vol de ces données il y a deux ans et n'a pas averti ses utilisateurs. C'est pour ça que je pense que nous ne pouvons pas leur faire confiance. »

« On n'a pas vraiment conscience de la valeur de nos données. C'est évident qu'elles sont utilisées à des fins publicitaires maintenant est-ce qu'elles sont utilisées à d'autres fins ? On ne sait pas vraiment. On n'a pas conscience des dérives. Il y a peut-être d'autres usages dont on n'a pas conscience. »

Quand nous leur demandons s'ils estiment que leurs données sont en sécurité (cf. question #5.3), beaucoup déclarent que non. Ces personnes font donc attention aux données qu'elles partagent :

« Peut-être que maintenant oui avec la mise en place du nouveau règlement européen, mais je pense que ce n'était pas le cas dans le passé avec Facebook. C'est pour ça que j'essaye de partager le minimum de données. Je ne partagerais pas mon numéro de compte bancaire par exemple même pas mon numéro de téléphone. »

D'autres nuancent et pensent que les informations partagées avec Google et Facebook ne sont pas critiques même s'ils estiment que cela peut avoir un impact pour certains:

« Non je pense que les données ne sont en sécurité nulle part. Mais d'un autre côté, aucune des informations que je partage avec Facebook n'est particulièrement sensible. Par exemple, ils savent quelle musique j'aime, les activités de loisirs que j'aime. Ce n'est pas la fin du monde si ces informations sont révélées.

Dans le cas du Brexit, si moi je reçois des publicités ciblées en faveur du Brexit cela ne va pas faire de différence pour moi par contre cela a eu une influence sur une partie de la population donc cela prouve que cela peut être dangereux. »

4.7.2. Protection des données personnelles

Quant à savoir si les entreprises en font suffisamment pour protéger nos données personnelles (cf. question #6), les réponses varient beaucoup. Pour ceux qui pensent que oui, il y a tout d'abord l'investissement consenti pour collecter ces données et le fait de garder un avantage compétitif :

« Je n'en sais pas suffisamment sur ce que ces entreprises font exactement avec mes données. Je pense qu'ils font beaucoup pour protéger nos informations tout simplement parce qu'ils ne souhaitent pas les partager avec leurs concurrents. Ils les protègent pour eux-mêmes et leur propre usage, car ils dépensent beaucoup d'argent pour les collecter. »

Les deux autres raisons invoquées concernent l'image et le respect des lois:

« Si elles le font, c'est peut-être pour deux raisons, la première c'est pour une question d'image. Pour l'instant ça commence à devenir un peu plus sensible comme sujet et puis, la deuxième raison c'est pour respecter les obligations légales avec l'entrée en vigueur du GPDR. Je pense qu'elles ne le font pas de gaieté de cœur. »

Ceux qui pensent le contraire mettent en avant une information trop peu compréhensible dans les règles générales d'utilisation ou le manque de sécurité des systèmes informatiques comme évoqué précédemment dans ce travail.

4.7.3. Vente de données

Toutes les personnes interrogées nous ont dit penser que leurs données personnelles sont vendues (cf. question #8).

« Oui je suis certain que ces informations sont vendues d'une manière ou d'une autre à des tiers. Ces données sont probablement anonymisées pour les traiter davantage. Je ne peux pas croire que Cambridge Analytica soit la seule affaire qui ait eu lieu ces dernières années. »

Plusieurs personnes pensent également que les récentes affaires telles que « *Cambridge analytica* » vont sensibiliser l'opinion et engendrer un changement dans la manière dont les entreprises traitent nos données.

« Je pense qu'ils vendent des données, mais avec tous les scandales qu'il y a eu avec Cambridge analytica a par exemple, je pense qu'ils se sont un peu calmés. »

Un autre déclare :

« Mais je suis certain qu'après cette affaire Facebook va modifier sa façon de travailler. »

4.7.4. Utilisation d'un pseudonyme

Seule une des personnes interrogées a indiqué utiliser un pseudonyme lors de ses achats en ligne :

« Parfois oui je change … évidemment pas l'adresse de livraison … mais le nom ou le prénom, ça oui parfois je change. Je mets même n'importe quoi. Parfois aussi je me crée des comptes Gmail que j'utilise pour des bêtes trucs comme ça. Je sais bien qu'ils vont m'envoyer des pubs par la suite et elles arrivent sur ce compte Gmail que je n'utilise que pour ça. »

Les autres disent ne pas en voir l'utilité et font suffisamment confiance aux sites d'achats en ligne auxquels ils s'adressent.

4.7.5. En résumé

Objectif #5: Est-ce que les personnes interrogées ont confiance dans le traitement de leurs données personnelles ?

La majorité des personnes interrogées estime ne pas être suffisamment protégée par les règles de Facebook et Google et ne leur fait pas confiance quant à l'utilisation de ses informations.

Par rapport à la protection des données personnelles, les réponses varient. Ceux qui pensent qu'elles sont en sécurité mettent en avant des questions d'image et de respect des lois. Ceux qui pensent le contraire pointent du doigt une sécurisation insuffisante des systèmes informatiques contenant ces informations.

De plus, l'ensemble des membres du panel pense que ses données personnelles sont vendues à des tiers.

Seule une personne déclare utiliser un pseudonyme lors de ses achats sur internet. Les autres faisant suffisamment confiance pour partager ces informations.

4.8. Objectif #6 : Connaissance des règles en vigueur sur la protection des données

Objectif #6: Quelle est la connaissance des personnes interrogées sur les règles de protection des données en vigueur actuellement ?
Questions #6 - #8 - #11 - #12

4.8.1. Connaissance des règles

Toutes les personnes interrogées ont entendu parler du GPDR ce qui n'est pas nécessairement le cas de l'ensemble de la population :

« Effectivement, j'ai entendu parler du nouveau règlement européen sur la protection des données. Par contre, l'autre jour je discutais avec des collègues pendant le temps de midi et j'étais surpris de les voir se poser des questions sur les e-mails qui leur demandaient d'approuver les nouvelles conditions d'utilisation de leurs applications. Ils n'avaient pas l'air au courant … »

Le niveau de connaissance des membres du panel est fort variable :

« Pour ce qui est du contenu des règles, je ne me suis pas encore penché dessus en détail. En fait, j'ai dû remplir pas mal de documents pour le boulot pour mon assurance médicale notamment, mais je ne connais pas les nouvelles implications en détail. »

D'autres en savent davantage :

« Le nouveau règlement s'assure que les sociétés ne stockent pas d'informations qu'elles ne doivent pas utiliser. Par exemple ne plus demander la date de naissance si ce n'est pas nécessaire. Et avec un peu de chance, les sociétés vont réduire la quantité d'informations qu'elles collectent au sujet des utilisateurs. Et en raison des amendes, les sociétés vont accorder davantage de moyens à la protection des données dont elles disposent. Pour ça je pense que ce nouveau règlement est une chose fantastique. Un désavantage est que cela pourrait empêcher l'avènement de nouvelles technologies dont on pourrait bénéficier, mais c'est un prix à payer pour la sécurité de nos données. »

La mise en place de ce nouveau règlement est vue comme une très bonne chose :

« Je ne connais pas vraiment ce que ça implique en pratique. Je crois que c'est quand même assez compliqué comme règlement, il y a beaucoup d'obligations. Les gouvernements au niveau européen se devaient de réagir aux différents scandales. C'est un peu une nécessité. Maintenant, est-ce que en pratique ça va vraiment protéger nos données ? Est-ce qu'il y aura un réel mieux pour l'utilisateur ? Est-ce que ce sera suffisant ? Ça on verra bien après.

Un des points positifs est que ça intervienne au niveau européen, que ce soit uniformisé …

Peut-être que ce règlement fera boule de neige et que les entreprises adapteront leurs règles en dehors de l'Union européenne sur base des règles en vigueur en Europe suite à cet exemple. Peut-être que d'autres pays se calqueront sur cet exemple et implémenteront le même type de règles qu'en Europe. »

Certains se posent des questions quant à l'application effective de ce nouveau règlement :

« Je pense que c'est une très bonne chose dans la mesure où le règlement est appliqué évidemment. La question que je me pose maintenant que cette loi est entrée en vigueur est la suivante : sera-t-elle vraiment appliquée. »

4.8.2. Règles en vigueur – règles indispensables à implémenter

Une des nouvelles règles les plus connues est le droit à l'oubli :

« Il y a le droit à l'oubli : chaque consommateur peut demander aux sociétés la liste des informations dont elles disposent à leur sujet et éventuellement demander que ces données soient effacées. »

« Je pense qu'une des règles c'est que tu peux à tout moment supprimer ton historique comprenant des données personnelles partagées dans le passé. C'est la règle la plus importante dont j'ai entendu parler mais je ne connais pas les autres règles. »

Parmi les règles indispensables à implémenter (question #12), beaucoup citent des règles qui font partie du GPDR, ce qui est plutôt une bonne chose :

« Dans le cas du supermarché, il faudrait qu'il y ait une notification qui indique que le centre commercial va utiliser nos données pour nous envoyer des notifications. Faire en sorte que le consommateur soit prévenu et au moins conscient parce que la plupart du temps ça se fait un peu dans notre dos. Prévenir que les données vont être utilisées et à quelles fins et puis aussi utiliser du vocabulaire pas trop compliqué … et puis aussi pas trop long … car si les conditions d'utilisation font 100 pages personne ne va les lire … Il faut que ce soit décrit en quelques lignes … sinon c'est comme s'il n'y avait pas d'informations, personne ne les lira. »

L'interdiction de la vente de données a également été avancée plusieurs fois :

« Comme règle indispensable à implémenter, je dirais simplement le fait de ne pas vendre les données à des tiers, je trouve que cette vente de données est contraire à l'éthique. Pour moi, ce serait la première chose. »

4.8.3. En résumé

Objectif #6: Quelle est la connaissance des personnes interrogées sur les règles de protection des données en vigueur actuellement?

Les personnes interrogées ont toutes entendu parler du nouveau règlement européen sur la protection des données. Certains connaissent une ou plusieurs règles, mais la majorité ne les connait pas.

Le droit à l'oubli a été cité à plusieurs reprises par les personnes au courant des règles en vigueur.

L'interdiction de vendre des données personnelles a été mentionnée plusieurs fois comme faisant partie des règles indispensables à implémenter. De même, une simplification de la description des conditions générales d'utilisation a été citée. Cette dernière fait d'ailleurs partie des nouvelles règles.

5. Conclusion

Dans le chapitre 1, nous avons décrit le grand champ d'application des techniques du « *Big Data* » et des gains considérables qu'une bonne utilisation de ces techniques peut avoir aussi bien pour les sociétés privées que pour les organismes publics. Ces techniques ne sont pas uniquement réservées aux grandes entreprises, elles sont mises à disposition de tout un chacun par Google et Facebook qui grâce à leurs plateformes de ciblage publicitaires 'Google AdWords' et 'Facebook Ads' qui permettent de segmenter et de cibler le marché en fonction de différents critères tels que l'âge, la position géographique, les centres d'intérêt, etc. Il en résulte un lien plus direct entre les consommateurs qui se voient proposer des produits en adéquation avec leurs centres d'intérêt et les entreprises qui peuvent mieux cerner les attentes du marché et proposer des produits attractifs.

La description évoquée au paragraphe précédent présente la situation idéale où consommateurs et entreprises bénéficient mutuellement de ces nouvelles techniques. La réalité peut parfois présenter une face plus sombre. L'actualité récente a en effet fait état de vol massif de données et d'utilisation de ces données à des fins politiques pour manipuler des élections via la diffusion de fausses informations auprès d'un public plus sensible à ce type de discours. Différents éléments de cet aspect plus inquiétant ont été évoqués dans le chapitre 2 avec, par exemple, l'enquête de tests achat montrant la vulnérabilité de certains objets connectés, la collecte abusive des données de localisation des clients utilisant le wi-fi dans un supermarché français, etc.

Dans le chapitre 3, nous avons rappelé les grands principes du nouveau Règlement Général sur la Protection des Données (RGDP) entré en vigueur en Europe le 25 Mai 2018. Celui-ci encadre désormais la collecte et le traitement des données à caractère personnel dans les 28 états membres de l'Union européenne.

Dans ce contexte, nous avons voulu savoir quelle était l'opinion de différents internautes par rapport aux données personnelles collectées lors de leur navigation sur Internet; sur Google et Facebook notamment. Pour cette étude quantitative, nous avons posé une vingtaine de questions ouvertes à 8 personnes de tranches d'âges et de professions différentes : de l'étudiant à la personne retraitée.

Cette étude a montré que les personnes interrogées étaient conscientes de l'utilisation de leurs données personnelles à des fins de marketing direct. Cette démarche est jugée comme peu dérangeante tant qu'elle n'implique pas de perte de temps et tant que les données utilisées sont peu sensibles. L'utilisation d'informations liées à la santé par exemple est très mal perçue. L'utilisation des données de géolocalisation n'est pas bien perçue également même si elle revêt certains aspects pratiques pour retrouver des amis lors d'un évènement par exemple.

Les personnes les moins favorables à l'usage de leurs informations personnelles se disent inquiètes, mais pas au point de ne plus utiliser les services en ligne. Elles sont conscientes qu'il s'agit du prix à payer pour bénéficier d'un service « gratuit » de qualité.

Nous ressentons d'ailleurs un manque de confiance par rapport à l'utilisation de leurs données personnelles : beaucoup soulignent un manque de transparence quant au traitement de leurs informations. Des conditions générales d'utilisations plus claires, plus courtes, plus lisibles les rassureraient sur ce point.

Le droit à l'oubli et à l'effacement des données est vu par beaucoup comme un aspect très positif du RGPD même si ces personnes s'interrogent quant au contrôle : comme s'assurer que ces données ont bien été effacées si la demande a été effectuée.

Les personnes interrogées ont toutes entendu parler du nouveau règlement (ce qui n'est pas forcément le cas de l'ensemble de la population comme le soulignait un de nos répondants). Certains connaissaient une ou plusieurs règles - d'ailleurs, le droit à l'effacement des données qui permet de demander de supprimer les données personnelles qu'une organisation possède à notre sujet est vu par beaucoup comme étant très positif - mais peu de personnes connaissaient les grands principes. Un travail de sensibilisation semble nécessaire à ce sujet.

D'ailleurs, l'étude de tests achats montrant la vulnérabilité des objets connectés (cf. chapitre 2) est vue comme une très bonne initiative. Les personnes interrogées se disent conscientes des risques associés à l'utilisation de ces objets. Plusieurs personnes ont mis en cause la responsabilité du fabricant quant à la sécurisation de ces objets. Elles estiment en effet que les fabricants devraient tester davantage leurs systèmes avant de commercialiser leurs produits. Paradoxalement, ces personnes ne seraient pas prêtes à payer davantage pour bénéficier d'une meilleure protection.

De même, plusieurs personnes ont pensé à la caméra de leur smartphone en entendant les résultats de cette étude. Ils estiment soit que le risque est minime soit que le risque est réel, mais moins pénalisant que le fait de se passer de son smartphone.

Beaucoup de personnes interrogées effectuent des achats en ligne, principalement pour l'aspect pratique et rapide. Certaines personnes seraient prêtes à partager davantage d'informations lors de leurs achats en ligne pour autant que cela n'occasionne pas de perte de temps, que ces questionnaires soient optionnels et que les questions posées ne soient pas jugées comme étant trop privées : des questions en lien avec les achats sembleraient acceptables.

En matière d'assurance peu de personnes interrogées accepteraient de partager des informations sur leurs trajets, leur vitesse, leur style de conduite pour bénéficier d'une réduction sur leur prime d'assurance. Le partage de la position GPS, le risque de perdre davantage que le gain engrangé sur la prime en cas d'excès de vitesse et le manque de confiance dans les compagnies d'assurance sont autant de freins à l'acceptation de ce système.

Même si la majorité des personnes interrogées estiment ne pas être suffisamment protégée par les règles de Google et Facebook et dit ne pas leur faire confiance quant à l'utilisation des informations personnelles, peu seraient prêts à payer pour bénéficier de ces services et éviter le partage de leurs informations. Seule une personne serait prête à le faire pour autant que ce montant ne dépasse pas quelques euros par mois. Le modèle actuel de partage de données semble donc convenir et les avantages perçus compensent largement les craintes évoquées même celles des personnes les plus inquiètes.

Une des perspectives futures de ce travail d'analyse serait d'étendre notre échantillon voire d'affiner certaines questions sur des sujets plus ciblés tels que les assurances, la sécurité des données, etc. afin d'approfondir l'analyse des résultats plus spécifiquement dans ces domaines.

Nous terminerons ce travail par une citation de Christpher Wylie, cet ancien directeur de recherches de la société « Cambridge Analytica » et lanceur d'alerte dans l'affaire du même nom qui résume bien la nature de la situation actuelle en matière d'utilisation de données personnelles:

« La question n'est pas comment aider les gens à rester anonymes ou comment empêcher les données personnelles d'être utilisées. C'est comment s'assurer que ces données sont utilisées d'une manière sécurisée pour le public. » *[41]*

Bibliographie

[1] Alexandra Simar. Peut-on rompre avec facebook et vivre heureux? *Le soir*, 2018.

[2] Filip Godelaine. Le paiement mobile, on y est! *Plus magazine*, 2018.

[3] John Rose, Olaf Rehse et Björn Röber. The value of our digital identity. *The Boston Consulting Group*, 2012.

[4] Marco Greco and Michele Grimaldim. What is big data? a consensual definition and a review of key research topics. In *AIP Conference Proceedings*, volume 97, page 1644, 2015.

[5] Larousse (https://www.larousse.fr).

[6] Robert Souza, Rob Trollinger, Cornelius Kaestner, David Potere, and Jan Jamrich. How to get started with big data. *The Boston Consulting Group*, 2013.

[7] The who, why and how of big data. Bain&Company Insight Infographic, 2015.

[8] Data strategy. Bain&Company (http://www.bain.com/consulting-services/advanced-analytics/data-strategy.aspx)

[9] Carrie Gates and Peter Matthews. Data is the new currency. In *Proceedings of the 2014 New Security Paradigms Workshop*, NSPW '14, pages 105–116, New York, NY, USA, 2014. ACM.

[10] Michael Blackburn, Jeffrey Alexander, J. David Legan, and Diego Klabjan. Big data and the future of R&D management. *Research-Technology Management*, 60(5):43–51, 2017.

[11] James Platt, Robert Souza, Enrique Checa, and Ravi Chabaldas. Seven ways to profit from big data as a business. *The Boston Consulting Group*, 2014.

[12] Nicolaus Henke, Jacques Bughin, Michael Chui, James Manyika, Tamim Saleh, Bill Wiseman, and Guru Sethupathy. The age of analytics: competing in a data-driven world. *McKinsey Global Insititute*, 2016.

[13]James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, and Angela Hung Byers. Big data: The next frontier for innovation, competition and productivity. *McKinsey Global Institute*, 2011.

[14] Nicolaus Henke, Ari Libarikian, and Bill Wiseman. Straight talk about big data. *McKinsey&Company*, 2016.

[15] David Court. Getting big impact from big data. *McKinsey&Company*, 2015.

[16] Helen Mayhew, Tamim Saleh, and Simon Williams. Making data analytics work for you - instead of the other way around. *McKinsey&Company*, 2016.

[17] Brad Brown and Josh Gottlieb. The need to lead in data analytics. *McKinsey&Company*, 2016.

[18] Rasmus Wegener and Velu Sinha. The value of big data: How analytics differentiates winners. *Bain&Company*, 2013.

[19] Facebook's global economic impact. A report for facebook. *Deloitte*, 2015.

[20] Facebook business - success stories: Actimel.
(https://www.facebook.com/business/success/actimel-france)

[21] Facebook business - success stories: Prêt à pousser.
(https://www.facebook.com/business/success/pret-a-pousser)

[22] Google adwords.
(https://adwords.google.com/intl/fr_be/home/how-it-works/)

[23] Rishi Bhandari, Marc Singer, and Hiek Van Der Scheer. Using marketing analytics to drive superior growth. *McKinsey&Company*, 2014.

[24] Alain Jennotte. La Belgique fait plier le géant Facebook. *Le Soir*, 17-18 Février 2018.

[25] Simon Souris. Facebook devra passer à la caisse en cas de non-respect du droit belge. *L'Écho*, 17-18 Février 2018.

[26] Perrine Signoret. Comment le centre-commercial des quatre temps a traqué ses visiteurs. *L'express/L'expansion*, 15 Juillet 2017.

[27] Perrine Signoret. Au BHV, et ailleurs, mieux vaut éteindre son téléphone pour éviter d'être pisé. *L'express/L'expansion*, 3 Août 2017.

[28] Martin Untersinger. Izly, l'appli du CNOUS qui géolocalise des étudiants et renseigne des sociétés publicitaires. *Le monde Économie*, 20 Octobre 2017.

[29] Une appli sportive dévoile les bases militaires américaines en Syrie et en Irak. *L'express/L'expansion*, 29 Janvier 2018.

[30] Géolocalisation et appli sportive: l'armée française rappelle ses troupes à l'ordre. *L'express/L'expansion*, 31 Janvier 2018.

[31] Commission nationale de l'informatique et des libertés (Cnil). Objets connectés: n'oubliez pas de les sécuriser!, Décembre 2017 (https://www.cnil.fr/fr/objets-connectes-noubliez-pas-de-les-securiser).

[32] Maison connectée, maison en danger! *Test achats*, 3 Mai 2018 (https://www.test-achats.be/action/espace-presse/communiques-de-presse/2018/hackable-home).

[33] Une maison connectée n'est pas à l'abris des hackers. *Test achats*, 3 Mai 2018 (https://www.test-achats.be/hightech/internet/news/maison-connectee).

[34] Internet of things research study. Technical report, HP Security Research, 2014.

[35] Lucie Ronfaut. Sécurité : la CNIL accuse deux jouets connectés d'atteinte grave à la vie privée des enfants. *Le Figaro*, 2017.

[36] Comment un téléviseur peut vous espionner. *Le Temps*, 7 Février 2017.

[37] Corentin DiPrima. Comment les partis utilisent nos données. *Le Soir*, 5 Avril 2018.

[38] Amaelle Guiton. Nationbuilder: aide-toi, le logiciel t'élira. *Libération*, 19 avril 2016.

[39] Martin Untersinger. Comment l'agence de propagande russe sur internet a tenté d'influencer l'élection américaine. *Le Monde*, 2018.

[40] Martin Untersinger. Comment une entreprise proche de Trump a siphonné les données de millions d'utilisateurs de Facebook. *Le Monde*, 2018.

[41] Sonia Delesalle-Stolper. Sans cambridge analytica, il n'y aurait pas eu de Brexit. *Libération*, 26 Mars 2018.

[42] Eric Brat, Stephan Heydorn, Matthew Stover and Martin Ziegler. Big data: the next big thing for insurers? *The Boston Consulting Group*, 2013.

[43] John Rose, Alexander Lawrence, and Elias Baltassis. Bridging the trust gap in personal data. *The Boston Consulting Group*, 2018.

[44] Réglement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016. (https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679)

[45] Fernand Letist. Touche plus à mes données! *Le vif*, (21):44–47, Mai 2018.

[46] Autorité de protection des données, https://www.autoriteprotectiondonnees.be/reglement-general-sur-la-protection-des-donnees.

[47] L'essentiel à connaître sur le GDPR/RGPD: définition, périmètre, principes et mesures, 2018.

[48] Elodie Lamer. Instagram attaqué devant la commission belge de la vie privée. *Le Soir*, pages 2–4, Mai 2018.

[49] Jean-Luc Giannelloni et Eric Vernette. *Etudes de marché*. Vuibert, 2015.