Université de Strasbourg

EM Strasbourg Business School

Master 2 E-Marketing et Management des TIC

Les données des consommateurs au cœur des technologies de l'Internet

Les facteurs d'adoption et d'utilisation des futurs objets connectés

Rédigé par

Jean-Christophe Mauss

Directrice de mémoire : Madame Jessie Pallud

Année Universitaire : 2015/2016

Remerciements

En préambule de ce mémoire, je tiens à remercier toutes les personnes ayant contribué à la réalisation de mon étude.

Je souhaite remercier Madame Jessie Pallud, ma directrice de mémoire, pour le temps et les conseils qu'elle m'a accordé.

Je tiens également à remercier Monsieur Jonathan Bitton, mon tuteur en entreprise, pour son accompagnement lors de mes recherches et le temps passé à la relecture de mon mémoire.

J'adresse également mes remerciements aux 500 répondants qui ont pris le temps de répondre à mon questionnaire et sans qui mon étude quantitative n'aurait pu avoir lieu.

Enfin, je tiens à remercier ma famille, mes amis, collègues et toutes les personnes qui m'ont aidé dans la réalisation de ce mémoire.

Table des matières

I. Introduction du sujet

L'Internet impacte considérablement notre manière de travailler, de communiquer, de nous informer et d'interagir dans un monde de plus en plus connecté. Dans les années 2000, la multiplication des communications et des échanges entre les différents acteurs de l'Internet a fait émerger un phénomène dépendant de cette mouvance, le big data. Il représente la masse informationnelle mondiale, initialement alimentée par le web, puis qui s'est vue approvisionnée par une nouvelle source de données issue des objets connectés. Combinés ensemble, l'Internet du web et l'Internet des objets forment l'Internet (B.Weinberg, 2015).

Par ce biais, les entreprises ont accès à un nombre grandissant d'informations. Elles collectent, partagent et accèdent aux données de leurs consommateurs et leurs comportements. La donnée est aujourd'hui essentielle pour les organisations et se retrouve souvent aux cœurs des futures stratégies digitales. Son analyse permet d'accéder à de nouveaux marchés, d'améliorer l'expérience client ou encore de créer de nouveaux produits et services.

En étant sur le web et en utilisant des objets connectés, les consommateurs laissent derrière eux une empreinte numérique de plus en plus importante et alimentent le big data, sans réellement savoir comment leurs données sont collectées et utilisées. D'après une enquête réalisée par Havas Media[1] en 2014, les consommateurs sont de plus en plus préoccupés par l'usage qui peut être fait de leurs données. En chiffres, 83,6% des interrogés sont inquiets de cette situation.

De nombreux organismes et auteurs soulèvent un problème d'éthique qui résulte de cette collecte de données. Cependant, la digitalisation de nombreuses entreprises et l'utilisation accrue de l'analyse numérique semblent faire partie d'un phénomène inévitable des années à venir. Deux visions s'opposent actuellement concernant le big data et la donnée consommateur : une vision utopique de ce traitement qui n'aurait pour but que d'améliorer

[1] Branche média d'Havas, 6ème groupe mondial de communication selon le classement Recma

l'expérience client et une vision dystopique avec le potentiel avènement d'un certain *Big Brother*[2] (McNeely et Hahm, 2014).

Les consommateurs font de moins en moins confiance aux entreprises qui ne communiquent pas par rapport à la collecte de données qui leur semble floue. Une question se pose alors : dans un contexte actuel de digitalisation des entreprises où la donnée est au cœur de tous les enjeux, sur quels leviers les entreprises devront-elles s'appuyer pour faire accepter leurs technologies et plus particulièrement les objets connectés ?

Les mots clés de ce mémoire sont : Big Data – Donnée consommateur – Internet des objets – Web – Tracking – Sécurité – Confiance client – Facteurs d'adoption

Avec cet avènement du big data et des technologies d'analyse, la donnée risque dans les années à venir de passer d'avantage concurrentiel à facteur clé de succès : les organisations auront besoin de la donnée consommateur. À travers ce mémoire, nous démontrerons que les organisations doivent miser sur la transparence et la confiance pour convaincre les consommateurs d'utiliser librement les technologies de l'Internet qui tendent à devenir de plus en plus intrusives.

Tout d'abord, nous analyserons le but de la collecte de données de la part des entreprises, les technologies associées et les limites légales. Ensuite, nous étudierons les impacts de cette collecte sur les individus. Nous utiliserons le cas de l'entreprise Disney qui utilise massivement les données clients dans son parc d'Orlando afin d'illustrer les bonnes pratiques concernant la collecte de données par objets connectés. Enfin, nous présenterons le modèle TAM (Technology Acceptance Model, David 1989) qui conclura la revue de la littérature et qui introduira la méthodologie.

Ainsi, nous effectuerons une étude quantitative en utilisant un modèle étendu du TAM sur une technologie de l'Internet des objets qui devrait avoir des impacts considérables lors de sa mise sur le marché : les pilules connectées développées par Google X (Alphabet). Cette technologie permettra de mesurer des changements biochimiques dans le corps humain. Ces changements peuvent être annonciateurs d'une tumeur, d'une crise cardiaque ou d'un

[2] Personnage de fiction du roman 1984 de George Orwell, Big Brother représente l'État policier et la perte des droits individuels de la population dans la culture populaire

accident vasculaire cérébral. Les particules seront ingérées via un comprimé et seront chargées de se fixer sur un type particulier de cellule tumorales. Ces dernières seront alors détectées et comptées grâce à un objet connecté (Les Echos, 2014). Sur quels facteurs devra se concentrer Google X pour faire accepter cette technologie à la population ?

Nous avons sélectionné cette technologie car il semble plus aisé pour une personne lambda de se projeter dans ce domaine relativement sensible qu'est la santé. Qui plus est, une étude de la Harvard Business Review de Thimothy Morey *« Customer Data : Designing for transparancy and trust »* démontre que nos voisins allemands et anglais accordent une très forte importance à leurs informations de santé. Nous espérons ainsi mettre en évidence que la confiance et la sécurité tiennent une place importante dans l'adoption de ce type de nouvelles technologies qui peuvent revêtir un caractère très personnel.

II. Revue de littérature

A. La collecte de données des consommateurs en entreprise

L'analyse et l'utilisation des données en entreprise n'est pas un phénomène récent. Internet a simplement permis de multiplier les échanges entre les individus grâce notamment grâce au web et aux objets connectés.

Ce nouveau volume de données en croissance depuis quelques années a introduit le phénomène de big data. Cette révolution que présente le big data est expliquée par quatre phénomènes, appelés les 4V (IBM, 2016) :

- La Variété des données : les données sont aujourd'hui de différente nature. Par le passé, la donnée était par essence « structurée ». Cela signifie qu'elle pouvait être stockée dans des tables, des bases de données relationnelles. Aujourd'hui, 80% des données circulant sont « non structurées » (exemple : photos, vidéos). Quand elles sont brutes, elles ne peuvent être classées dans des tables. Il est cependant possible de les traiter grâce à des technologies dans le but de les convertir dans une forme de données structurées.
- Le Volume des données : en 2014, la quantité de données stockées dans le monde atteignait près de 7 zettaoctets (7 000 milliards de gigaoctets) alors que seulement 0.5% de cette quantité était analysée. En 2010 il fallait 2 jours pour produire 5 exaoctets (5 milliards de gigaoctets) alors qu'en 2003, il aurait fallu 60 ans. Entre 2009 et 2011, plus de 90% des données mondiales ont été créées (Redfern 2011). En 2018, 44 zettaoctets de données devraient être produites (Le Monde, 2016).
- La Vitesse des données : fait référence à la vitesse à laquelle les données sont créées et partagées.
- La Véracité des données : correspond à la qualité des données, si ces dernières sont justes, dignes de confiance ou erronées (rumeurs ou diffusions malveillantes sur les

réseaux sociaux, capteur défectueux, etc.). Le large volume de données permet généralement de pallier le potentiel biais des erreurs.

IBM ajoute un 5ème V qui correspond à la valeur, au potentiel économique et stratégique que l'entreprise va pouvoir extraire de ces données.

Le concept de big data peut être scindé en trois différentes perspectives qui présentent des opportunités et des défis (Nunan et Di Domenico, 2013) :

- La première est de répondre aux problèmes technologiques de stockage, de sécurisation, d'analyse et de faire face au volume toujours grandissant de données collectées ;
- La seconde se focalise sur la proportion de la valeur commerciale qui peut être attribuée aux informations à l'issue des analyses. Ce concept est né du fait de l'émergence de technologies d'analyse de plus en plus performantes et de l'augmentation du partage d'informations personnelles de la part des consommateurs ;
- La troisième relève de l'impact sociétal du big data et plus particulièrement de son impact sur la vie privée des individus.

Le volume important du big data le différencie principalement des « données d'entreprises » qui étaient jusque-là utilisées pour faire de l'analyse. Le big data est trop volumineux pour un serveur d'entreprise, trop déstructuré pour de classiques bases de données relationnelles et trop rapide pour les data-warehouses et bases de données classiques (Davenport, 2014). De nouvelles technologies émergent pour faciliter le traitement de ces informations mais les organisations doivent avoir recours à des experts de l'analyse de données, les data scientists, pour traiter et manipuler les informations issues du big data. La donnée est centrale dans cette analyse et apporte une nouvelle approche de la prise de décisions que nous allons détailler.

1. Le but de cette collecte

a) Les différents courants d'utilisation

De nos jours, certaines organisations ont plus recours au big data que d'autres. Tom Davenport décrit quatre catégories d'organisations en fonction du rapport qu'elles entretiennent avec le big data :

- *Big data competitors* : cette catégorie désigne les organisations ayant accès à un très large volume d'informations concernant leurs activités opérationnelles et leurs clients. Ces dernières utilisent de manière intensive leurs données. Exemple : firmes d'investissement.
- *Overachievers* : ces organisations ont un accès limité aux données mais sont dévouées à les utiliser autant que possible dans le but de soutenir leurs prises de décisions. Exemple : l'industrie des biens de consommation et certains départements opérationnels.
- *Underachievers* : ces derniers ont un accès à une vaste quantité de données mais n'en tirent pas de réel avantage. Exemple : opérateurs télécom.
- *Disadvantaged* : ces organisations ont un accès limité à l'information et tirent donc rarement profit de cette dernière dans leur prise de décision. Exemple : entreprises du domaine de la santé.

Cet accès à l'information va cependant être exacerbé du fait de l'évolution de l'Internet des objets. Le terme a été définit pour la première fois par Kevin Ashton[3] en 1999 comme étant un système où l'Internet est connecté au monde physique par l'intermédiaire des capteurs omniprésents tels que les RFID. Les prédictions quant à la prolifération des objets connectés sont d'actualité. Gartner (2014) prévoit une évolution de 0.9 milliards d'unités en 2009 à 26 milliards d'unités d'ici 2020, Cisco prévoient quant à un seuil de 50 milliards pour la période (voir figure n°1).

La quantité d'informations provenant des consommateurs et de leurs multiples sources d'accès à l'Internet est en croissance. Les organisations cherchent alors à collecter ces

[3] Kevin Ashton est le cofondateur du centre de recherche Auto-ID au MIT (Massachusetts Institute of Technology)

informations dans le but de les analyser et d'optimiser leurs performances. Thomas Davenport identifie quatre principaux champs d'action de cette collecte de données pour les entreprises : leur analyse doit permettre aux entreprises de faire des économies, d'optimiser les routines quotidiennes, de prendre de nouvelles décisions et de développer de nouveaux produits et services. D'un point de vue du consommateur, la collecte de données a pour principal objectif la création de valeur (Erevelles, Fukawa, et Swayne, 2016).

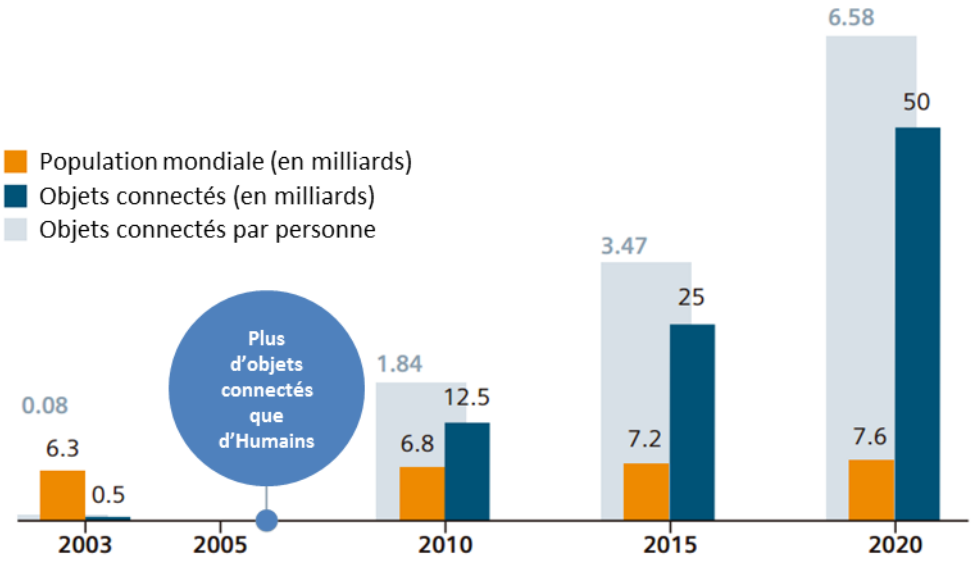


Figure n° 1 : La croissance des objets connectés d'ici 2020 (Cisco IBSG, avril 2011, paru dans Pictures of the Future, The Magazine for Research and Innovation, automne 2012)

b) Prise de décisions et création de valeur

Sunil Erevelles a publié un article dans le Journal of Business Research en juillet 2015 concernant l'impact de l'analyse numérique sur la transformation du marketing. Il fonde son article sur la théorie de l'avantage concurrentiel par les ressources (*Resource-based theory,* Birger Wernerfelt) qui a été utilisée par de nombreux chercheurs ces dernières années (Barney, 2014 et Day, 2014). Il y introduit le phénomène de big data et décrit ainsi son impact sur le marketing (voir figure n°2).

Selon la théorie de l'avantage concurrentiel par les ressources, ce sont les ressources d'une entreprise, aussi bien tangibles qu'intangibles, et la manière dont l'entreprise les mobilise, qui permettent son développement et sa capacité à créer un avantage concurrentiel. L'avantage concurrentiel est donc considéré comme inhérent à l'organisation.

Les ressources de l'entreprise peuvent être physiques (sites de production, machines disponibles, stock...), humaines (le nombre de salariés, leur niveau de qualification...) et organisationnelles (système d'information, contrôle de la qualité, procédures...) (Barney, 1991). Dans son article, Sunil Everelles classifie les différentes ressources dans un contexte de big data. Les ressources physiques désignent ainsi l'infrastructure de collecte, de stockage et d'analyse. Les ressources humaines font référence aux data scientists et aux différents autres postes stratégiques qui savent quelle information collecter, comment la collecter et surtout de quelle manière la traiter. Enfin, les ressources organisationnelles désignent les processus internes qui doivent permettre de répondre aux attentes des consommateurs (Viane, 2013).

Pour conserver leur avantage concurrentiel, les entreprises doivent sans cesse s'adapter au marché grâce à leurs capacités dynamiques (Teece, 2007). Pour David Teece, les capacités dynamiques désignent « *la capacité d'une firme à reconfigurer sa base de ressources pour faire face aux changements de l'environnement* ». La capacité d'une entreprise à répondre au changement (capacités dynamiques) est possible dès lors que cette dernière tire profit de ses compétences et de ses connaissances internes pour créer de la valeur. La masse d'informations clients que de nombreuses entreprises possèdent apparait ici comme une source riche d'information pour déceler des changements dans l'environnement. Une entreprise s'appuyant sur cette information pour déceler un besoin non satisfait de son consommateur met toutes les chances de son côté pour créer de la valeur et améliorer ses capacités dynamiques.

Southwest Airlines a utilisé un logiciel d'analyse pour étudier les conversations entre son personnel et ses clients. Grâce à l'outil, la compagnie aérienne a pu déceler quelles étaient les questions les plus posées et quelles étaient les attentes clients qui n'étaient pas satisfaites. L'entreprise a développé ses ressources organisationnelles grâce au logiciel et a pu enrichir grâce à son application les capacités de ses ressources humaines en proposant de nouvelles formations à son personnel. Par l'étude du capital informationnel disponible en interne, Southwest Airlines a pu adapter son offre de services et ainsi satisfaire certains besoins de ses clients qui étaient jusque-là non détectés.

D'un autre côté, les entreprises doivent être capables de capturer les signaux en provenance du marché et ainsi avoir les capacités de prédire et de s'adapter à la demande (capacité d'adaptation) (Day, 2011). George Day développe le concept de capacités d'adaptation dans son article « Closing the marketing capabilities gap » paru en 2011. Les capacités d'adaptation se distinguent des capacités dynamiques de par leur caractère exogène à l'entreprise. L'entreprise qui développe des capacités d'adaptation est donc capable de capturer des signaux externes à l'entreprise pour adapter son offre.

Données / **Orientation**	**Exploitation**	**Capacités développées**	**Exemple**
Interne ➔ Externe	Ressources internes à l'entreprise	Capacités dynamiques	Southwest Airlines
Externe ➔ Interne	Ressources externes à l'entreprise, écoute du marché	Capacités d'adaptation	Target

Tableau n°1 : Capacités dynamiques et capacités d'adaptation (Day, 2011)

Les capacités d'adaptation sont bien souvent liées à la structure organisationnelle de l'entreprise qui permet de développer ce type de compétences. La capacité d'adaptation relève de la faculté de l'organisation de déceler des tendances de marché et d'ainsi positionner son offre (Ma, Yao, et Xi, 2009). Quand les données du big data en provenance des consommateurs sont bien exploitées, ces dernières peuvent créer des opportunités pour les organisations et améliorent leurs capacités d'adaptation (Banker, 2014).

En 2012, Target a ainsi réussi à prédire le comportement de ses consommateurs grâce au big data. L'entreprise a réussi à déceler le fait qu'une consommatrice soit enceinte ou non, et sa date d'accouchement prévisionnelle en fonction de son panier d'achat. Target utilisait des techniques de marketing prédictif au profit de ses capacités d'adaptation au marché.

L'entreprise a utilisé cette information pour influencer ces femmes enceintes en leur proposant des biens relatifs aux nourrissons avant ses concurrents et initiait potentiellement ainsi une relation de fidélité sur le long-terme (Duhigg, 2012).

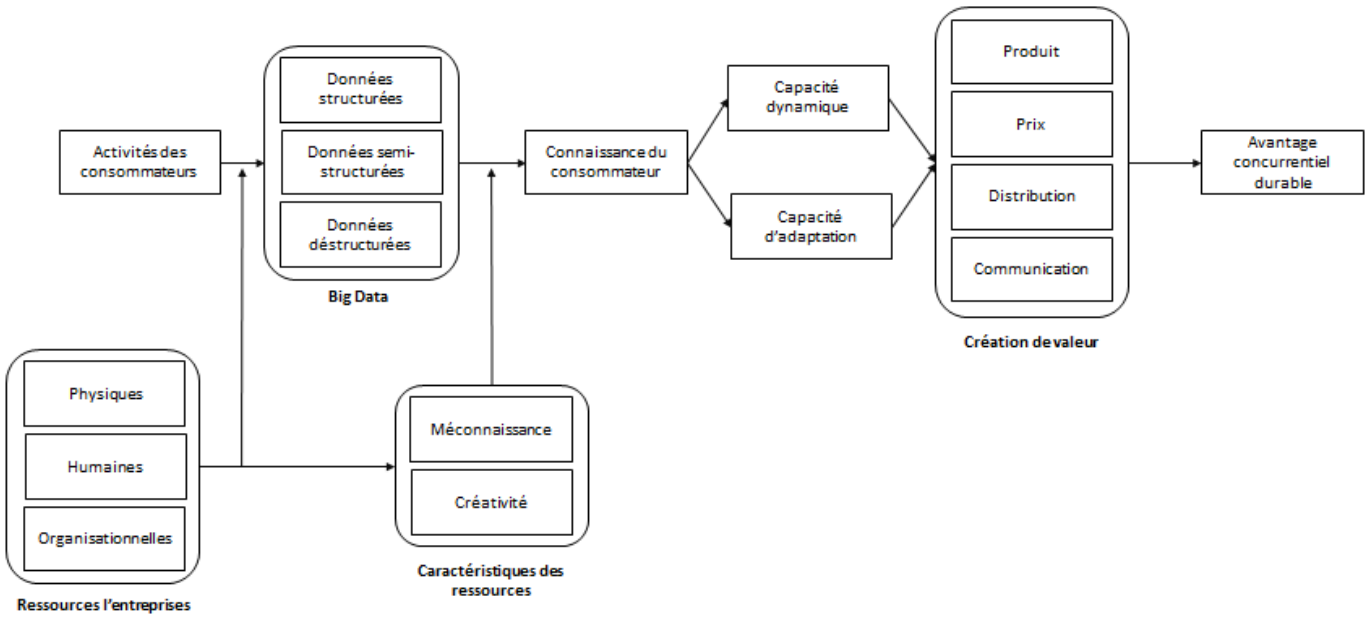


Figure n°2 : Théorie de l'avantage concurrentiel par les ressources grâce au big data (Everelles et al. 2016)

L'une des limites de la théorie de l'avantage concurrentiel par les ressources est l'origine de ces différentes ressources de l'entreprise. Cette théorie est développée par Jay Barney en 2014. C'est pourquoi le concept de « méconnaissance » est introduit dans la théorie. Le but de la recherche est d'acquérir des connaissances. La recherche implique alors d'admettre que l'on ne sait pas quelque chose, que l'on a une méconnaissance d'un certain domaine ou d'une activité. Proctor et Schiebinger avancent que « comprendre que l'on ne *sait pas* quelque chose (ou plus communément appelé « méconnaissance »), est aussi important que de comprendre ce que l'on sait ». Ainsi, les entreprises qui admettent avoir certaines lacunes en termes de connaissances et qui permettent une certaine latitude à leurs employés en matière de créativité favorisent l'émergence de nouvelles idées et facilitent ainsi la recherche. Les techniques d'analyses associées au big data doivent ainsi permettre aux chercheurs de déceler de nouveaux modèles mathématiques et de découvrir de nouveaux phénomènes sans pour autant s'appuyer sur des connaissances acquises. Dans ce contexte, une perspective basée sur « la méconnaissance », et donc la recherche, permet

potentiellement plus de découvertes qu'une perspective basée sur les connaissances déjà acquises (Anderson, 2008).

La connaissance a ses limites alors que l'ignorance n'en a pas (Firestein, 2012). Everelles ajoute donc le concept de méconnaissance comme une caractéristique des ressources de l'entreprise. Si une organisation accepte le fait d'avoir des lacunes en matière de connaissance et cherche à inverser le phénomène en transformant cette méconnaissance en connaissance, la vitesse de création de connaissances ne sera qu'exponentielle. De plus, si la méconnaissance est considérée comme une caractéristique des ressources de l'entreprise, cette dernière est très compliquée à imiter pour les concurrents.

La créativité d'une entreprise est également essentielle pour tirer tout le plein potentiel du big data et des données de ses consommateurs en créant de nouvelles activités marketing. Sans côté innovateur et créatif, les entreprises rencontreront de la difficulté à élargir leur champ d'activité marketing et à intégrer le big data dans leurs activités. Tout comme la méconnaissance de l'entreprise, les capacités créatives d'une organisation sont difficilement imitables pour les concurrents (Erevelles, 2007).

Les capacités dynamiques et les capacités d'adaptation alimentées par les différentes ressources de l'entreprise permettent alors la création de valeur en influençant les quatre variables initiales du marketing mix que sont le produit, le prix, le lieu de distribution et la communication *(Product, Price, Place, Promotion.).* La création de valeur résulte alors en un avantage compétitif temporaire ou potentiellement durable en fonction des cas (Ambrosini et Bowman, 2009).

- Produit : pour faire face à la concurrence, Ford a utilisé les données collectées de millions de véhicules à travers le monde. Après avoir analysé les données relatives à la commande vocale, Ford a détecté que le bruit ambiant dans l'habitacle perturbait la reconnaissance vocale. Cette découverte a permis le développement d'un réducteur de bruit et le repositionnement du microphone dans le véhicule (King, 2012). Le big data a ici permis l'innovation produit sans attendre des recommandations émanant d'outils de recherche marketing traditionnels (Satel, 2014).

- Prix : une stratégie de prix flexible s'adaptant à la loi de l'offre et de la demande dans le but d'optimiser ses profits est possible grâce au big data (Steinbach, 2012). Cela a été le choix stratégique de la Major League de Baseball. Des facteurs additionnels se sont ajoutés aux taux et vitesses de ventes. Ainsi, la Ligue tenait compte du lieu de match, du classement des équipes, de la météo, du « bruit » sur les réseaux sociaux, etc. C'est en combinant ces différents facteurs que la Ligue pouvait estimer combien un individu était prêt à dépenser pour une place et un match donné.
- Distribution : Amazon utilise toutes ses données clients pour optimiser sa stratégie de distribution. L'entreprise tient compte de l'historique de vente, de recherche, et de l'activité du panier de son consommateur pour prédire le moment où ce dernier va effectuer son achat et ainsi commencer le processus de livraison avant même la complétion de la commande (Banker, 2014).
- Communication : la communication de messages va pouvoir être optimisée grâce notamment à la géolocalisation des individus. Il est aujourd'hui possible de déduire quelle sera la prochaine destination d'un individu grâce aux informations géo-spatiales. Il est ainsi possible d'optimisation un message pour un consommateur en fonction de sa prochaine destination et ainsi guider son achat (Sadilek et Krumm, 2012).

Nous avons ainsi vu l'importance de la donnée consommateur pour les organisations et la manière dont ces dernières peuvent en tirer profit. Nous allons maintenant nous intéresser au processus de collecte de ces informations.

2. Les technologies de collecte associées

a) Internet : environnement web et environnement objets connectés

Les technologies liées à l'Internet évoluent rapidement depuis son émergence dans les années 1990. À l'origine, lors de l'arrivée du web (aussi appelé web 1.0), l'information était statique et à sens unique. L'entreprise poussait l'information vers le consommateur, et ce dernier n'avait pas la possibilité de rentrer en contact avec l'entreprise par le web. Dans les années 2000, le web 2.0 a permis une diffusion de l'information de manière plus

dynamique. Les consommateurs pouvaient communiquer avec les entreprises par l'intermédiaire du web, et ce sous de nombreuses formes et sources. Naissaient ainsi les blogs, les tweets, les likes, les partages de vidéos et photos, etc. (Kaplan et Haenlein, 2010). Les réseaux sociaux ont exacerbé le partage de données de la part des consommateurs et ces derniers partagent de plus en plus d'informations relatives à leurs habitudes de consommation et à leur vie privée.

De nos jours, la démocratisation des objets connectés entraîne une hausse des données partagées encore plus considérable entre les différents acteurs de l'Internet. Les termes « objets connectés » caractérisent un large champ de technologies mais peuvent être classés en six grandes catégories en fonction de leur champ d'application (voir tableau n°2).

Les wearables • Divertissement • Fitness • Smart watch • Localisation et tracking	**Domaine de la santé** • Maintenance prédictive • Automatisation des soins conférés aux patients • Suivi des prises de médicaments • Contrôle d'accès
Constructions et domotique • Contrôle d'accès • Régulation de la lumière et des températures • Optimisation de l'énergie • Maintenance prédictive	**Industries intelligentes** • Optimisation des processus • Inventaires en temps réel • Contrôle des ressources • Maintenance prédictive • Sécurité des employés
Villes intelligentes • Contrôle de la circulation • Caméras de surveillance • Optimisation de l'éclairage public	**Automobile** • Divertissement et informations • Alerte pneumatiques • Maintenance prédictive • Communication voiture/voiture

Tableau n°2 : classification des technologies de l'Internet des objets par champ d'application (Adaptation Texas Instrument)

De nombreux appareils sont connectés à l'Internet et réceptionnent ou transmettent des données : les ordinateurs, les serveurs, les smartphones, les tablettes et d'autres appareils que les consommateurs utilisent aujourd'hui pour naviguer sur le web. Cependant, les objets connectés doivent se distinguer de ces appareils car ces derniers ont la particularité de communiquer directement avec l'Internet. Les objets connectés permettent la connexion directe du monde physique à l'Internet (Weinberg et al. 2015). Il est donc nécessaire de

distinguer les deux univers qui forment aujourd'hui l'Internet avec d'un côté un environnement basé sur le web, et un autre basé sur les objets connectés (voir figure n°3).

Dans l'environnement web, ce sont les consommateurs qui sont à l'origine de la création de la donnée du fait de leurs actions. Les données collectées reflètent alors les « comportements en ligne dans un monde en ligne » du consommateur (Weinberg et al. 2015). La donnée peut être de différents types : textes, images, vidéos, clics, cookies, etc. Ces données sont générées ou entrées par le consommateur. Elles sont affiliées à un comportement sur le web et généralement utilisées par une organisation et ses partenaires commerciaux pour adapter leurs offres en fonction d'un comportement passé.

Dans l'environnement des objets connectés, les appareils contrôlent et enregistrent les comportements du consommateur dans le monde physique dans lequel ce dernier interagit. Un thermostat connecté va ainsi réguler la température d'une pièce en fonction du comportement et des préférences d'un consommateur. Ce dernier n'a plus besoin de participer activement sur l'appareil pour qu'il collecte, analyse et traite les données. Dans ce type d'environnement, les données sont partagées entre l'objet connecté et son fournisseur mais aussi entre les différents appareils. Ainsi, lors d'une chaude journée, une voiture connectée peut directement communiquer l'heure d'arrivée d'un consommateur au thermostat connecté se trouvant dans son logement pour ainsi optimiser le réglage de la température des différentes pièces en fonction de ses préférences et de ses habitudes (Weinberg et al. 2015). L'apprentissage a donc lieu en fonction des actions en temps réel et ce sont les appareils qui prennent les décisions.

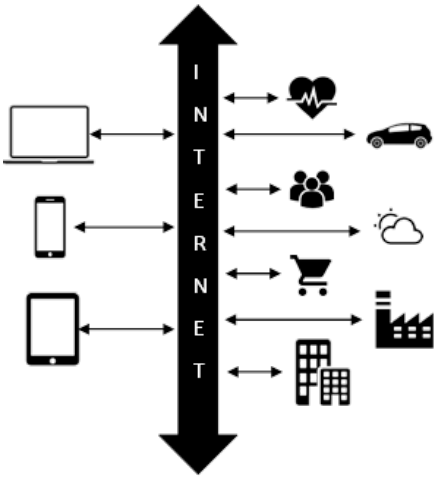


Figure n°3 : Alimentation de l'Internet par le web et les objets connectés

Bruce Weinberg propose un tableau récapitulatif des principales distinctions qui sont faites entre la perspective de l'Internet du web et celui des objets d'un point de vue de la donnée.

La donnée et les processus associés	**Web**	**Internet des objets**
Donnée	La donnée est en ligne, digitale. L'environnement et le contexte sont bâtis par les organisations	La donnée est originaire du monde physique et fluctue en fonction des différents contextes dans lequel interagit le consommateur
Enregistrement de la donnée	De manière active, par le consommateur	De manière passive, par les appareils
Partage de la donnée	Avec d'autres fournisseurs	Avec d'autres appareils
Apprentissage	En fonction des actions en ligne	En fonction des actions dans le monde réel
Prise de décision	Par les organisations, en fonction des actions passées, moins en temps réel	Par les appareils, de façon dynamique et en temps réel

Tableau n°3 : principales distinctions entre un environnement web et un environnement des objets connectés (Adaptation Weinberg et al. 2015)

Nous vivons une période de transition d'un environnement de l'Internet web à un Internet englobant web et objets connectés. Les entreprises tirent profit de la donnée consommateur sur le web grâce à des procédés de collecte obscurs et bien souvent à l'insu

des utilisateurs. C'est pourquoi nous allons nous intéresser à ces processus et les détailler avant d'analyser ceux des objets connectés.

b) La capture de données sur web

Les multiples organisations collectant des informations sur les consommateurs sur le web peuvent être classées en différentes catégories selon la relation qu'elles entretiennent avec eux, et la quantité d'informations récoltée. Bien souvent, la collecte de données a lieu sans que l'individu concerné soit au fait de cette action (Loftus, 2011). Les sites web peuvent ensuite transmettre ces informations à des entreprises spécialisées dans l'affiliation, vendre ces données à des agrégateurs ou autoriser certaines entreprises de tracking à placer leurs pixels sur leur page (Martin, 2014). Les différentes organisations peuvent être classées suivant deux axes : en abscisse le type de relation entretenue avec l'utilisateur (Bedi, 2013), et en ordonnée la quantité d'informations collectées.

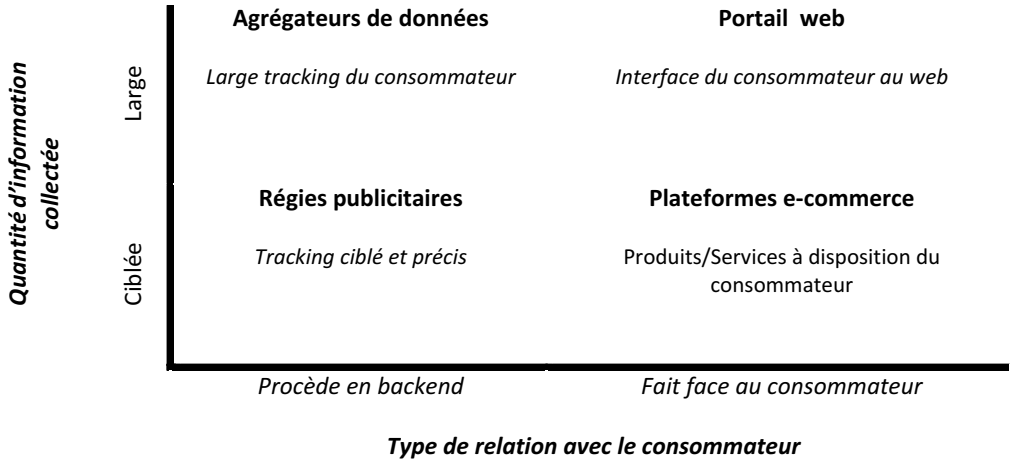


Figure 4 : Catégorisation des collecteurs de données en ligne en fonction de la quantité d'information collectée et de la relation avec le consommateur

(1) Richesse de l'information collectée

Les entreprises peuvent collecter énormément d'informations sur leurs consommateurs. En allant dans les conditions de respect de la vie privée d'une société spécialisée dans l'agrégation de données clients (Axciom), nous pouvons lire que cette dernière possède *« noms, adresses, e-mails, numéros de téléphone, des données démographiques et socio-comportementales »* qui sont collectées *« par le biais de ses questionnaires papier et en ligne, de promotions, ses partenaires commerciaux, des sources publiques, des bases de*

données commercialisées ainsi que nos sites Web ». Cela signifie que les informations sont collectées, stockées et bien souvent échangées entre les différents acteurs du web. Le caractère sensible, privé et personnellement identifiable de la donnée est très contextuel (Nissenbaum, 2009).

En reprenant les différents acteurs vus en figure n°4, nous pouvons décrire les quatre types d'entreprises collectant des données sur les consommateurs en ligne (Martin, 2014) :

- Les portails web : ces derniers entretiennent une relation directe avec les consommateurs mais collectent et agrègent des données issues de multiples contextes ;
- Les sites de vente en ligne : ils font face aux consommateurs et collectent de l'information à leur sujet dans un contexte précis ;
- Les agrégateurs de données : ils collectent, stockent et revendent des données sur les consommateurs. Ces données sont issues de nombreuses sources en ligne mais peuvent également trouver leur source dans le monde physique (appel téléphonique, questionnaire) ;
- Les régies publicitaires : ils n'ont pas de rapport direct avec le consommateur et revendent des données sur les consommateurs à des clients pour que ces derniers ciblent leurs publicités. Ces régies sont souvent appelées des AdExchange. Le contexte de collecte est souvent spécifique et limité dans le temps.

Ces entreprises collectant des informations sur les internautes le font de trois manières différentes (Lancelot-Miltgen et Lemoine, 2015) :

- De manière directe : l'entreprise sollicite l'internaute par le biais d'un formulaire ;
- De manière indirecte : l'entreprise achète ou loue une base de données de sociétés spécialisées ou obtient des données déclaratives auprès de clients ;
- De manière discrète : des données sont collectées par le biais de techniques non directement décelables par l'internaute (techniques de tracking). Ce sont ces dernières que nous allons maintenant analyser.

(2) Technologies de collecte discrète

Aujourd'hui, les technologies de collecte de données sur le web permettent de considérablement enrichir les bases de données de profils consommateurs (Angwin et McGinty, 2010). Nous allons ici développer les trois principales technologies de tracking que sont les cookies, les pixels et l'empreinte digitale des navigateurs. Ces technologies ont pour principal but la compréhension de comportements sur le web et la mise en place de campagnes marketing plus ciblées.

Les cookies sont encore aujourd'hui la technologie de collecte la plus utilisée sur le web. Il faut distinguer deux types de cookies : les cookies internes au site et les cookies de tiers. Le principal but d'un cookie interne est d'identifier un utilisateur afin de lui permettre de reprendre sa visite à l'endroit où il avait quitté le site sans l'obliger à retaper ses identifiants, et potentiellement personnaliser sa page d'accueil.

Lors d'une première visite sur un site web, un utilisateur peut être amené à remplir un formulaire d'inscription en fournissant des informations personnelles (un nom, un prénom, une adresse email, une adresse physique, etc.) qui sont ensuite stockées dans un cookie, lui-même stocké dans le navigateur. Des données relatives aux actions de l'utilisateur sont ainsi enregistrées dans le navigateur et seront recherchées par le site lors de la prochaine visite grâce à l'implémentation d'un identifiant d'utilisateur dans le fichier cookie. Cet identifiant permet d'associer de multiples visites et interactions à un même utilisateur (Felten et Schneider, 2000). Si nous prenons l'exemple d'une navigation sur un site e-commerce, le cookie permet de ne pas à avoir à se reconnecter à son compte à chaque changement de page.

Les cookies dit « de session » sont supprimés à la fermeture du navigateur et ne collectent pas d'informations qui permettent d'identifier l'individu. Les cookies « permanents » quant à eux sont stockés sur l'appareil jusqu'à échéance de leur date d'expiration ou de leur suppression par l'internaute. Les cookies permanents sont utilisés pour identifier un utilisateur, analyser son parcours de navigation et personnaliser son interface.

Le cookie stocke donc de l'information dans le navigateur de l'internaute. Cette information se présente sous la forme d'une suite de chiffres et de lettres. De base, le cookie n'a besoin

que de se souvenir du navigateur d'un internaute. La plupart des cookies peuvent contenir des informations plus personnelles sur les individus de manière cryptée si ces derniers en ont bien entendu fourni au site (What are Internet cookies and what do cookies do?, 2008).

Cette description relative aux cookies correspond aux cookies internes. Les cookies de tiers sont des cookies déposés par des régies publicitaires ou des agrégateurs de données et permettent de suivre le parcours de navigation d'un internaute sur le web. Les informations collectées permettent de dresser des profils d'individus et de segmenter la population. Les organisations peuvent alors vendre leurs bases de données ou proposer des prestations de service de ciblage pour adapter et optimiser les messages marketing. En allant sur le site du Monde (http://www.lemonde.fr/) et grâce à l'outil Lightbeam de Firefox, nous pouvons observer que 59 cookies de tiers ont été déposés sur la machine. Les tiers sont par exemple : cedexis.com, smartadserver.com ou encore facebook.com (voir figure n°5).

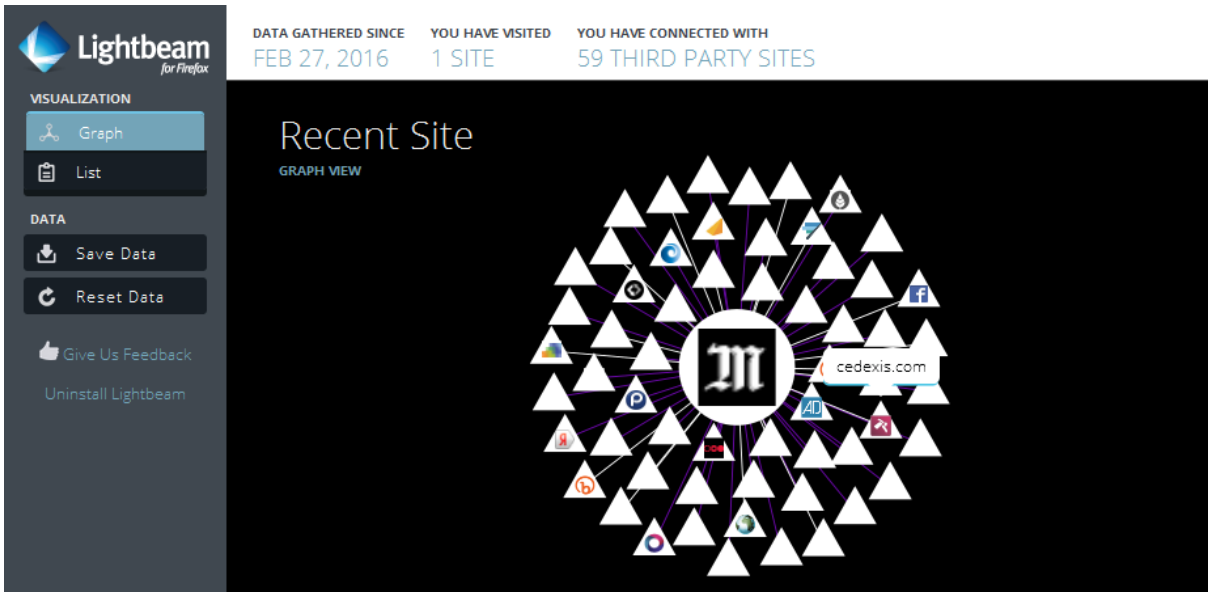


Figure n° 5 : 59 cookies de tiers sur le site du Monde

Les super cookies sont considérés comme des évolutions des cookies. Ils sont stockés de manière permanente sur la machine de l'utilisateur. Cela permet à des entreprises comme Google et Facebook de collecter plus de données sur leurs utilisateurs et de revendre ces dernières car ces cookies sont quasiment impossibles à supprimer (Ring, 2015).

Les web beacons, ou plus communément appelés pixels, sont utilisés en complément des cookies. Ces pixels sont des images au format GIF de 1 pixel implémentées dans le code HTML de sites web ou d'emails. Les pixels permettent de suivre les interactions d'un utilisateur sur une page, l'impression de publicités ou encore l'ouverture d'emails (Angwin, 2010).

Les organisations placent les pixels dans le code HTML de pages web pour tracer le comportement des internautes et les impressions de publicités. Lorsqu'une page contenant un pixel est chargée, le pixel va devoir appeler le serveur de stockage pour être chargé. Cet appel permet donc aux entreprises concernées de savoir que leur page a été chargée. Cette technologie est fréquemment utilisée lors de l'envoi d'emailing pour savoir si ces derniers ont été ouverts. Bien souvent lors de l'appel au serveur, un cookie est déposé sur l'appareil de l'internaute (Cookies, tags and Pixels: Tracking customer engagement, 2015).

Même sans cookies et sans pixels, il est possible de recréer le profil d'un internaute. L'Eletronic Frontier Foundation (EFF), spécialisée dans la préservation des données personnelles donne la définition de l'empreinte digitale d'un navigateur. Cette méthode permet de tracker un utilisateur et plus particulièrement son navigateur par le biais de ses configurations, options, système d'exploitation, adresse IP et extensions. Lors de la visite d'un site web ces informations sont envoyées au serveur. Cette technique est possible grâce aux « tags JavaScript » qui consiste à placer du code JavaScript dans les pages HTML qui enregistre les événements voulant être mesurés (García, Martín, et Aubert, 2012). Les techniques de fingerprint ont été adoptées par de nombreux sites en complément de leurs cookies pour tracer les utilisateurs. Des entreprises telles que Google ou Twitter l'affichent dans leurs règles de confidentialité : « *Nous recueillons des données propres à l'appareil (comme le modèle de l'appareil, la version du système d'exploitation, les identifiants matériels uniques)* » ; « *Ces prestataires de service tiers collectent des informations envoyées par votre appareil dans une requête de page Web* ». En 2010, Eckersley a analysé l'empreinte digitale de 470 161 navigateurs. Après avoir analysé les données, il s'est avéré que 83,6% des navigateurs avaient une empreinte unique.

Après avoir détaillé les principaux processus de collecte de données sur le web et leurs différents acteurs, nous allons maintenant nous intéresser à la collecte de données via les objets connectés.

(3) La capture de données via les objets connectés

Comme vu précédemment, l'Internet des objets collecte des informations relatives au monde physique. Une fois collectées, ces informations subissent une opération de transmission avant de finalement être traitées et utilisées. Nous allons ici nous concentrer sur la phase de collecte d'information de la part des objets connectés.

À la différence du web, l'utilisateur d'un objet connecté sait que l'objet, de par sa nature, va collecter des données. Nous allons détailler les techniques actuellement utilisées dans ce processus. Comme pour le web, plusieurs techniques sont utilisées et seront certainement amenées à évoluer dans les années à venir.

La création de données se fait par le biais de technologies de captation rattachées à des capteurs, des appareils photos, des caméras, des GPS. La collecte des données a lieu par le biais de technologies de communication à courte distance (Bluetooth, NFC). La technologie RFID joue un rôle crucial dans l'Internet des objets. Cette technologie permet d'identifier des objets ou des individus, de stocker de l'information les concernant et de transférer cette dernière à d'autres appareils électroniques. Le système RFID fonctionne grâce à deux composants. Le premier est un « tag » qui est fixé à l'objet, composé d'un circuit intégré et d'une puce, permettant ainsi d'identifier l'objet grâce à un identifiant unique (UII, Unique Item Identifier) et de stocker de l'information. Une antenne permet la transmission des informations contenues dans la puce vers le deuxième élément essentiel à la technologie RFID : le lecteur. Ce lecteur permet de collecter des données en provenance du tag pour ensuite les transmettre sur Internet. Il existe deux types de tags RFID, un passif et un actif. Le système de RFID passif utilise un tag qui doit être détecté par un lecteur RFID à proximité pour lire et transmettre les informations. L'actif quant à lui (aussi appelé beacon) est équipé d'une batterie et peut par conséquent opérer et communiquer sur de plus grandes distances.

Une autre technologie jouant un grand rôle de collecte dans l'Internet des objets est celle des capteurs sans fils (Wireless Sensor Networks). Ces capteurs permettent l'agrégation et le traitement de données de très nombreux domaines allant de celui de la surveillance à celui de la santé. Ces capteurs sont généralement déployés pour mesurer un phénomène spécifique comme une hausse de température par exemple. Le principal défaut de cette technologie est son manque d'efficience en matière de durée de vie de la batterie.

La technologie NFC (Near Field Communication) permet à des appareils de partager de l'information entre eux lorsque ces derniers entrent en contact ou se trouvent à proximité. Le NFC est souvent utilisé pour partager des informations personnelles (contacts, photos, vidéos) ou encore pour réaliser des transactions. La technologie peut être vue comme une évolution de la RFID dans le sens où elle s'en inspire mais permet en plus la communication bidirectionnelle.

L'un des challenges actuel pour les entreprises est de réussir à tirer profit de cette collecte de données dans les deux environnements, web et objets connectés, et ce en les faisant communiquer entre eux. Certaines entreprises peuvent profiter de cette opportunité pour cibler et toucher de façon plus précise leurs prospects et cela de façon pertinente. Par exemple, une entreprise spécialisée dans la vente de logements pourrait placer des beacons (environnement objets connectés) dans ses différents biens. Si un prospect est à la recherche d'un logement sur leur site web (environnement web) et abandonne le processus avant l'objectif fixé (bien souvent une demande de contact), les informations concernant les caractéristiques du bien pourraient être sauvegardées. Au passage à proximité du logement à caractéristiques correspondantes, un message ciblé et personnalisé serait envoyé au prospect. L'environnement web communique avec l'environnement des objets connectés grâce aux données collectées, c'est ici le cookie web qui peut déclencher le beacon.

Après avoir détaillé les principales techniques de collecte de données consommateur sur l'environnement web et celui des objets connectés, nous allons maintenant nous intéresser à la législation en vigueur.

3. Les réglementations en vigueur

L'innovation et l'évolution du numérique vont plus vite que l'élaboration des nouvelles normes législatives (Bensoussan). Cela représente un enjeu en termes de droit des entreprises et des individus. Les données personnelles des individus sont directement ou indirectement liées à une réglementation, les lois s'empilent les unes sur les autres.

a) La CNIL

La CNIL (Commission Nationale Informatique et Libertés) est une autorité administrative française chargée de veillée à ce que l'informatique soit au service du citoyen. Elle exerce depuis le 6 janvier 1978 suite à la divulgation de la « Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ». Il est important de noter que la CNIL se soumet aux décisions de la Cour de Justice de l'Union Européenne qui exerce une politique de protection des données personnelles pour les pays de l'Union Européenne. Néanmoins, chaque pays peut apporter des réglementations supplémentaires en fonction des spécificités de sa juridiction.

La CNIL accompagne les professionnels dans leur mise en conformité et protège les particuliers vis-à-vis de leurs données personnelles. La CNIL a également un rôle de veille en ce qui concerne l'impact des innovations technologiques sur les libertés individuelles des individus et leur droit à la vie privée. L'organisation a quatre missions principales (*CNIL : nos missions*, 2016) :

- Informer/Protéger : la CNIL informe tant les professionnels que les particuliers quant à leurs interrogations sur le domaine du numérique et notamment de la collecte de données. Toute personne peut s'adresser à la CNIL si elle éprouve des difficultés à faire valoir ses droits.
- Accompagner/Conseiller : la CNIL accompagne les organisations et met à leur disposition des instruments leur permettant de se mettre en conformité au cadre législatif en vigueur. Pour de nombreuses grandes entreprises souhaitant aller plus loin dans le traitement des données personnelles, la CNIL conseille par exemple l'embauche d'un correspondant informatique et libertés (CIL) ou l'adhésion à des packs de conformité/référentiels sectoriels.

- Contrôler/Sanctionner : les contrôles de la CNIL ont lieu en entreprise ou en ligne et permettent de vérifier la mise en place concrète de la loi en vigueur. Ainsi, la CNIL est autorisée à accéder à tous locaux professionnels, à demander la communication de tout document nécessaire au contrôle, à accéder aux différents programmes informatiques (données comprises) et à recueillir les renseignements utiles à son investigation. À l'issu de contrôles, la CNIL peut décider des mises en demeure.
- Anticiper : la CNIL a également une mission de veille pour rester au fait de l'émergence de nouvelles technologies pouvant impacter les droits et la vie privée des individus. Un laboratoire lui permet d'effectuer des expérimentations sur des produits et applications innovants. Des experts externes sont parfois amenés à donner leur avis et à contribuer au programme annuel d'études.

Les quatre missions s'appliquent à la protection de la personne physique et ce même dans le cadre de son activité professionnelle. La personne physique doit être distinguée de la personne morale (société, organisation, association, etc.) qui n'est pas protégée par la loi informatique et libertés. La loi protège la personne physique dans le cadre du traitement automatisé ou non de ses données personnelles.

Selon la loi, une donnée à caractère personnel désigne toute information relative à une personne physique identifiée ou qui permet de le devenir. Par exemple, nom, prénom, date de naissance, adresse postale, adresse électronique, numéro de téléphone, sont considérés comme des données à caractère personnel (article 2 al. 2).

Il est intéressant de souligner que la CNIL considère l'adresse IP comme étant une donnée à caractère personnel mais que ce n'est pas le cas de toutes les juridictions (Caprioli, 2012). L'adresse IP peut être considérée comme une suite de chiffres se rapportant à un ordinateur et non pas à un utilisateur, ce qui ne rend donc pas la donnée directement nominative.

b) Obligations du responsable du traitement

Le traitement de la donnée personnelle implique tout type de manipulations de l'information : collecte, organisation, conservation, modification, consultation, etc. (article 2 al. 3). C'est sur le responsable du traitement de la donnée qu'incombe le respect de la loi de 1978 (article 3-1) : il doit définir les finalités de traitement et les moyens mis en œuvre. Le

sous-traitant n'est pas responsable du traitement de la donnée si ce dernier est effectué sous les instructions du responsable (Article 35). Toute personne traitant des données à caractère personnel pour le compte d'un responsable de traitement est considérée comme un sous-traitant.

Les données personnelles ne peuvent être collectées qu'en respectant certaines conditions. En effet, elles doivent être collectées de manière licite, pour des finalités déterminées, explicites et légitimes. Les données doivent donc servir dans un but précis, il n'est pas autorisé de collecter trop de données uniquement pour un usage futur non déterminé. Les données doivent être uniquement conservées pour une durée n'excédant pas la durée nécessaire aux finalités du traitement (article 6 – 1,2,3,4,5).

Le responsable de traitement des données doit adopter les mesures de sécurité physiques (des locaux) et logiques (du système d'information) pour garantir la sécurité des données et leur confidentialité. Seules les personnes autorisées peuvent avoir accès aux informations collectées. Les destinataires doivent être explicitement désignés pour obtenir leur communication.

Le responsable du traitement des données doit également permettre aux individus concernés d'exercer leurs droits. Ces droits concernent le droit à l'information, à l'accès, à la rectification et à l'opposition.

En ce qui concerne le droit à l'information, le responsable du traitement des données doit communiquer son identité, la finalité du traitement, les destinataires des informations, l'existence de droits, et les transmissions envisagées à des tiers. Tout individu a un droit d'information sur les fichiers le concernant si ce dernier est fiché par une organisation (article 39 – I). En principe, les individus sont informés de la collecte de leurs données personnelles par le biais de mentions obligatoires et aussi par des chartes de confidentialité.

Les individus étant fichés par une entreprise et justifiant de leur identité ont droit d'accéder à l'intégralité des informations collectées (article 40). La personne qui en fait la demande a le droit de connaître la finalité des traitements engendrés, le type de données enregistrées, l'origine de ces données, les éventuels transferts de données hors Union Européenne et a le

droit d'obtenir des explications concernant les procédés informatiques ayant contribués à d'éventuels scorings (article 39 – I)

Toute personne a le droit de s'opposer pour un motif légitime à ce que ses données personnelles subissent un traitement (article 38). Ce droit d'opposition ne s'applique pas dans le cadre légal où une autorité gouvernementale légitime souhaite procéder à un traitement.

Le droit à la rectification permet à un individu de rectifier, mettre à jour, compléter ou effacer des données personnelles le concernant si ces dernières sont inexactes, incomplètes ou périmées (article 40). L'individu peut par exemple refuser de répondre à certaines questions d'un questionnaire si ces dernières ne sont pas obligatoires.

Il est interdit de collecter et traiter des données à caractère personnel qui laissent apparaître de manière directe ou non, les origines ethniques de l'individu, ses opinions politiques, philosophiques et religieuses, ainsi que les données qui sont relatives à la santé ou à l'orientation sexuelle d'un individu (article 8-1). Certaines finalités de traitement exigent cependant la collecte de ce type de données personnelles comme certains objets connectés (article 8-2). Par exemple, le bracelet Fitbit permet d'évaluer son état de santé physique, et ces données doivent être collectées et traitées pour permettre l'utilisation de l'objet.

c) Droit à l'oubli

L'une des craintes des individus concernant leurs données personnelles est que ces dernières puissent se retrouver sur la place publique de l'Internet : le web. Les moteurs de recherche sont un passage obligé lorsqu'un individu souhaite y accéder. Un individu peut avoir un contenu le concernant sur le web et regretter l'indexation de ce dernier (*Les moteurs de recherche*, 2016). L'individu doit alors s'adresser au webmaster du site concerné, ou directement au moteur de recherche pour obtenir son déréférencement (*Le droit au déréférencement*).

Le groupe de travail des CNIL européennes (G29) veille à ce que le droit à l'oubli défini par la Cour de Justice de l'Union Européenne soit respecté sur le web. Par l'arrêt C-131/12 du 13

mai 2014, la Cour de justice de l'Union européenne confirme que tous les moteurs de recherche sont responsables du traitement des données personnelles et doivent par ce fait respecter le droit à l'oubli.

Par souci de transparence, Google a mis en ligne en février 2016 une page dédiée aux demandes de déréférencement dans l'Union Européenne *(Impact de la vie privée sur les résultats de recherche*, 2016). Depuis le lancement de la procédure en 2014, Google a reçu près de 400 000 demandes de suppression concernant près de 1 400 000 URL. Après détermination de l'intérêt public ou non de la requête, 42,6% des URL ont été supprimées.

La CNIL menaçait Google d'une amende jusqu'en février 2016 par rapport à ce droit à l'oubli. La société avait bien déréférencé des dizaines de milliers d'URL suite à la demande de citoyens français sur les extensions européennes du moteur de recherche. Cependant, les résultats étaient toujours disponibles sur les autres extensions géographiques. Par exemple, un lien déréférencé sur Google.fr ne l'était pas sur Google.com (*Droit au déréférencement : Rejet du recours gracieux formé par Google à l'encontre de la mise en demeure*, 2015). Google estimait que le déréférencement au niveau mondial était un frein à la liberté de circulation des données. La firme a cependant infléchi sa position en désindexant les liens sur Google.com si la connexion au moteur de recherche se fait depuis une machine basée en Europe (*Google fait un pas vers le « droit à l'oubli » réclamé par l'UE*, 2016).

d) Transfert de données hors Union européenne : les États-Unis

Dans un cadre d'internationalisation des communications et des échanges, les transferts de données hors de France et hors Union européenne ne cessent de croître. Il est important de noter que les transferts de données à caractère personnel hors de l'Union européenne sont interdits sauf si le pays destinataire a une réglementation permettant de suffisamment garantir un niveau de protection adéquat.

La CNIL met à disposition des entreprises certains outils permettant d'apporter un niveau de sécurité suffisant aux données personnelles en leur possession : modèles de règles internes ou encore clauses contractuelles types.

Depuis le 6 octobre 2015, il n'est plus possible de transférer des données personnelles vers les États-Unis sur la base du « Safe Harbor ». Depuis 2000, l'accord était en place car l'Union européenne jugeait que les États-Unis présentaient des garanties suffisantes en termes de protection des données personnelles. Dans son rapport rendu en octobre 2015, la Cour de justice de l'Union européenne estimait que le « Safe Harbor » n'était plus conforme au droit européen du fait notamment des systèmes de surveillance de masse américains (Ducourtieux, 2015).

Un nouvel accord de principe, le « Privacy Shield », a été annoncé le 2 février par la Cour de justice de l'Union européenne. Ce nouvel accord sera plus protecteur des droits européens et entrainera de nouvelles obligations pour les entreprises. À noter que ce sont les entreprises américaines privées qui doivent, de manière individuelle, se soumettre au « Privacy Shield » et que ce n'est pas l'État américain qui change ses lois (Eudes, 2016).

B. L'impact sur les individus

La collecte de données sur les individus est grandissante. Le web a été la première interface digitale qui a permis cette collecte, puis s'en est suivie l'émergence de l'Internet des objets. Ces nouvelles technologies permettent de collecter de nouvelles informations sur les individus et leurs comportements dans le monde physique. La collecte de données du consommateur est devenue centrale dans le processus de création de valeur et d'amélioration de l'expérience client (Everelles, 2016, Morey, 2015). Le thermostat de l'entreprise Nest, filiale d'Alphabet (maison mère de Google), ajuste automatiquement le niveau de chauffage et de climatisation de ses clients en fonction de leurs habitudes de consommation.

Le perpétuel flux croissant d'informations a permis l'amélioration et l'optimisation de nombreuses industries comme celle de la santé, de l'environnement et des villes intelligentes. En 2015, la société Uber, spécialisée dans le transport individuel de personnes, a partagé avec la ville de Boston les données relatives aux trajets de ses clients. La ville peut ainsi fluidifier son trafic dans la zone urbaine en adaptant les horaires de ses divers transports et peut également prioriser les travaux sur la chaussée (*Uber to share ridership data with Boston - the Boston globe*, 2015). Le big data présente donc de nombreuses

sources d'opportunités pour les entreprises et les individus, autant qu'il présente des limites.

1. Les avantages : qu'attendent les consommateurs

De manière générale, les consommateurs apprécient le fait que la collecte de données leur permette l'accès à des produits et services de meilleure qualité ou de faire des économies. Dans l'environnement web par exemple, Google et Facebook utilisent les données consommateurs pour optimiser les résultats de recherche de leurs applications. En ce qui concerne les objets connectés, leur prolifération est en train d'entraîner une quantité croissante de la donnée consommateur. D'après une étude du cabinet Gartner, 6,4 milliards d'objets connectés devraient être utilisés dans le monde en 2016, c'est une hausse de 30% par rapport à 2015. Le nombre d'objets connectés devrait atteindre 20,8 milliards d'ici l'horizon 2020 (Van der Meulen*, Gartner*, 2016).

Thimothy Orey et al. ont réalisé une étude auprès de 900 panélistes en 2014 et ce dans cinq pays différents (États-Unis, Grande-Bretagne, Allemagne, Chine et Inde). L'un des buts de cette étude était de mettre en lumière ce que les consommateurs attendent en retour de la collecte de leurs données, tout environnements confondus. Dans le cadre de cette étude, l'équipe s'est concentrée sur trois utilisations des données par les entreprises : améliorer un produit ou un service, optimiser les campagnes de communication marketing de manière ciblée et la revente de ces informations.

Lorsque les données collectées servent à l'amélioration d'un produit ou d'un service, les consommateurs retrouvent généralement un équilibre dans la transaction par le biais de cette amélioration. En revanche, ils attendent plus de valeur en retour lorsque leurs informations sont utilisées dans le cadre de campagnes marketing, et de manière encore plus significative lorsqu'elles sont revendues. D'après leur étude, si les données sont utilisées pour améliorer une expérience, deux tiers des utilisateurs sont prêts à, et parfois même veulent, partager leurs informations en échange de ce bénéfice. L'application de Google, « Google Now », prend en compte une multitude de sources de données pour améliorer l'expérience de son utilisateur : emails, calendrier, localisation, loisirs et autres

sources d'information sont analysées pour personnaliser l'interface et les messages envoyés à son propriétaire.

Les consommateurs attendent des bénéfices notables et immédiats de cette collecte de données (Weinberg et al.*).* L'environnement de l'Internet des objets est particulièrement marqué par ce côté instantané de la réponse à la collecte. L'entreprise Zipcar, spécialisée dans la location de véhicules, a par exemple été parmi les pionnières dans son industrie à équiper ses véhicules de la technologie RFID. Ses clients peuvent localiser un véhicule à louer via l'application mobile, le réserver, l'utiliser et payer automatiquement pour les frais en fin de service via cette même application. L'entreprise s'est ainsi constituée un avantage concurrentiel vis-à-vis de la concurrence tout en améliorant l'expérience client (Brink, 2015).

Un autre avantage de l'Internet est la possibilité de contrôler et d'accéder à tous les appareils qui y sont reliés. Cela permet au niveau individuel l'optimisation d'un service (accès à un cloud personnel, connexion à un réseau câblé à distance) tout comme au niveau de la population de manière générale comme dans les villes intelligentes ou le domaine de la santé.

L'Internet transforme les villes du monde entier. La collecte de données est réalisée par le biais de nombreux facteurs et leur traitement futur peut être bénéfique à la population de manière générale. En matière de mobilité, la collecte exercée par les objets connectés aux véhicules ou les smartphones des conducteurs peuvent permettre l'optimisation des feux de circulation ou guider les individus vers les stationnements libres les plus proches de leur localisation, en accord avec leurs habitudes de consommation (Borgia, 2014).

La distribution d'énergie dans la ville peut également être optimisée grâce à l'analyse de données collectées. Les divers bâtiments des villes sont équipés de multiples capteurs et objets intelligents (smartphones, ordinateurs portables, télévision, caméras de surveillances, thermostats, etc.) qui collectent des données et permettent des utilisations dans différents domaines. Cela concerne par exemple le domaine de la sécurité (gestion des accès, détection d'intrusion), de la maintenance qui est bien souvent préventive, et de l'automatisation de services comme l'éclairage ou l'irrigation.

Les États tirent également parti de cette collecte de donnée dans les villes intelligentes pour garantir la sécurité de l'ordre public. Les actions doivent permettre la maintenance des infrastructures, la prévention des risques et la protection des individus (Borgia, 2014).

Le domaine de la santé est fortement impacté par la collecte massive de données. Les objets connectés permettent de mesurer et contrôler en temps réel un grand nombre de facteurs des patients (température, pression sanguine, niveau de cholestérol, rythme cardiaque). Dans *« The Quantified Self Fundamental Disruption in Big Data and Biological Discovery »* Mélanie Swan nous explique qu'il y a une tendance proactive de la part des individus à collecter des informations les concernant pour pouvoir ensuite agir en conséquences. Nombreuses sont les personnes qui mesurent et analysent leur poids, leur énergie, leur qualité de sommeil ou toutes autres performances athlétiques. Cette tendance se développe notamment grâce aux objets connectés qui permettent cette collecte de données sur l'environnement et les actions des individus. Ce phénomène lié au big data touche les individus et modifie leurs usages du quotidien.

De façon générale, les individus pensent contrôler leurs données personnelles. Cependant de nombreuses limites et enjeux découlent de la multiplication des sources de données personnelles des individus.

2. Les limites

Que cela concerne l'environnement web ou celui des objets connectés, de nombreux auteurs soulèvent des limites quant à la collecte de données d'un point de vue éthique.

a) Environnement web

Les pratiques des entreprises concernant le traitement de données personnelles (PI, personnellement identifiables) ou non-personnelles (ne permettant pas d'identifier personnellement un individu) ne sont pas claires pour de nombreux individus. D'après une étude menée par Lorie Faith Cranor et al. en 2014, de nombreuses entreprises font le choix de rester silencieuses aux vues des utilisations des données de leurs consommateurs. Ce flou autour de la donnée peut tromper les individus.

Kirsten Martin décrivait les acteurs de la collecte (figure n°4) et les a classés en trois rôles soulevant des questionnements éthiques quant à leurs actions. Les acteurs peuvent être membres d'une chaîne logistique de la donnée, avoir un rôle de surveillance ou d'aide à l'application de la loi (voir figure n° 5).

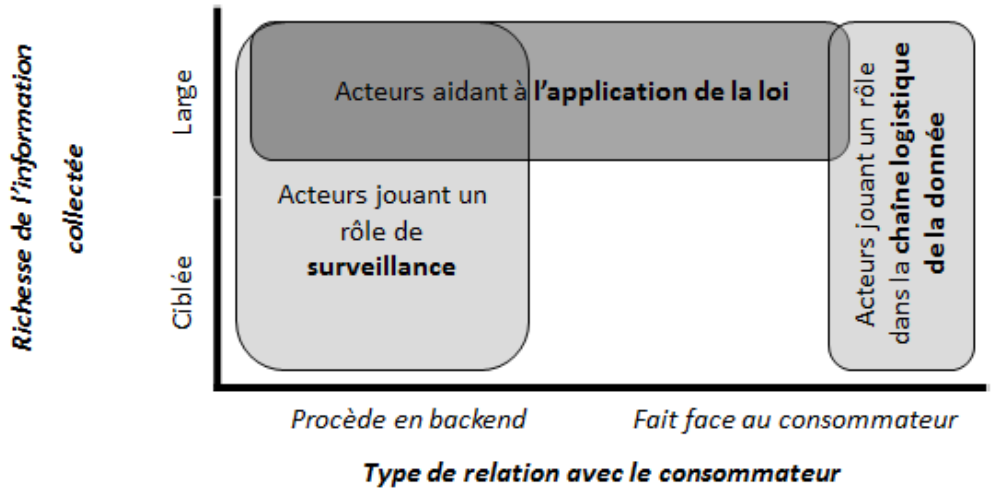


Figure 5 : Rôle des acteurs collectant les données (Martin 2014)

Lorsqu'une organisation fait partie d'une chaîne logistique de l'information en ligne, cette dernière est amenée à transmettre des données à d'autres organisations. Par exemple, un utilisateur peut confier des informations à un site web, qui peut transmettre ces informations à une entreprise spécialisée dans le tracking, qui pourra elle aussi transmettre ces données à des agrégateurs. Les agrégateurs revendent ensuite ces données consolidées à des organisations souhaitant cibler un certain segment d'individus. Une chaîne logistique de la donnée est alors créée. Toutes les actions en ligne sont enregistrées, elles peuvent ensuite être consolidées, puis revendues (Nissenbaum, 2011). De plus, les sites web améliorent au fil des années leurs capacités techniques de traçage des actions individuelles (Loftus, 2011).

Kirsten Martin soulève deux problèmes émanant de cette chaîne logistique de la donnée. L'information transmise peut potentiellement avoir des conséquences négatives sur des individus ou groupes d'individus, et les données transmises pourraient violer les politiques de confidentialité du point de vue du consommateur.

La revente ou transmission d'informations à des tiers peut potentiellement porter atteinte aux consommateurs (Mitchell, 2012). Par exemple, les données pourraient donner lieu à des modifications de primes d'assurance ou de taux d'emprunts (Tene et al., 2012). Des adolescents pourraient également se voir recommander des publicités relatives à des programmes de régime ce qui ne ferait qu'exacerber cette peur présente chez les jeunes (Angwin, 2010). Plus que la sensibilité apparente de la donnée (financière, médicale), ce sont les conséquences et potentielles nuisances qui doivent être évaluées lors de la transmission d'informations à des tiers (Etzioni, 2012). Un large champ d'informations peut être utilisé avec parfois de graves conséquences pour les individus (Martin, 2014).

Les données collectées par un site web sont soumises à des politiques de confidentialité. Partager ces informations avec des tiers peut tromper l'utilisateur au regard de ses attentes en terme de vie privée. En se rendant sur le site d'une agence de voyage et en achetant des billets d'avion, un consommateur peut s'attendre à se voir proposer des offres de logement sur place. Ce dernier ne s'attend cependant pas à ce que ses informations soient transmises à des agrégateurs de données, que ses informations soient stockées pendant des années et utilisées à des fins de pricing (Martin, 2014). En se rendant sur un site web et en interagissant avec, un utilisateur passe un contrat de confiance implicite avec l'organisation (Heeney, 2012).

Les organisations font parfois partie d'un vaste système de surveillance. Ce concept se réfère au fait qu'aucune action en ligne n'est pas tracée par un ou plusieurs organismes. Le problème soulevé est que les individus n'ont pas la possibilité de choisir avec qui ils désirent ou non partager leurs informations. Ce principe de surveillance est contradictoire avec le besoin des individus de ne pas se sentir observés (Benn, 1984). L'activité en ligne des individus est une extension de leur activité hors ligne (Nissenbaum, 2011). Le sentiment d'être observé est particulièrement exacerbé lorsque les individus ont la sensation de ne pas pouvoir éviter la surveillance, et lorsqu'ils ne savent pas qui l'exerce (Cohen, 2008). L'agrégation de données sur toutes les plateformes en ligne et dans de différents contextes d'utilisation permettent aux entreprises d'avoir des descriptions précises de leurs clients. Le bénéfice de la personnalisation des produits et services proposés aux clients ne sera peut-être pas proportionnel vis-à-vis des données collectées. Plus la collecte de données est importante et plus cette dernière est individualisée, plus les agrégateurs de données

peuvent en tirer profits. Ces données permettent à ces entreprises de créer de la valeur (Martin, 2014). Pour limiter ce rôle de surveillance, les entreprises collectant des données à l'insu des consommateurs devraient se montrer plus visibles et accessibles.

Enfin, les organisations peuvent joueur un rôle en aidant à l'application de la loi. Les États peuvent être amenés à consulter des entreprises dans le but d'accéder à des données collectées en ligne et pouvant aider à la sûreté de l'État. En 2012, les services de sécurité américains ont fait près de 8500 demandes à Google pour obtenir des données sur des utilisateurs. Google a coopéré dans 88% des cas (Kelly, 2013).

En 2016, le FBI a demandé à Apple de créer un outil de déverrouillage permettant de déchiffrer l'IPhone de l'un des auteurs de l'attaque de San Bernardino. L'entreprise a refusé en argumentant que la création d'un tel outil pourrait être préjudiciable aux détenteurs d'IPhones : l'outil pourrait être utilisé à des fins d'espionnage. Le conflit opposant Apple au FBI est arrivé au Parlement français en mars 2016. Les amendements présentés n'ont pas abouti mais la séance a permis le débat. Il est reproché par certains ministres un manque d'accès aux données pour permettre de contrer des menaces. Jean-Jacques Urvoas, ministre de la Justice avance cependant que *« Nous ne sommes pas aveugles. Nous avons accès aux flux, là où nous avons des difficultés, c'est le stock »*.

Les amendements présentés à l'Assemblée Nationale avaient pour but d'affirmer la suprématie de l'État et obliger les entreprises à coopérer avec ce dernier dans le cadre d'enquêtes terroristes par tous les moyens. Le Gouvernement français souhaiterait que la décision soit prise au niveau international ou à minima au niveau européen pour avoir plus de poids face aux géants de l'Internet. Les dispositifs de chiffrement mis à disposition des utilisateurs ont été mis en place suite aux révélations d'Edward Snowden en 2013 quant à l'espionnage de masse de la NSA. L'encryptage des données est-il un dispositif sécuritaire ou un argument commercial ? Des ministres partagent le point de vue que des entreprises comme Apple ne défendent « pas les intérêts de la liberté mais les intérêts commerciaux » (Reynaud, 2016).

Rendre les données plus obscures, moins claires à déchiffrer, a pour conséquence de donner moins de valeur à ces informations. C'est ce que préconisaient en 2011 Brunton et

Nissenbaum dans leur article « *Vernacular Resistance to Data Collection and Analysis: A Political Theory of Obfuscation*. »

b) Internet des objets

La donnée personnelle et son traitement sont essentiels à l'environnement de l'Internet des objets. L'Internet des objets n'existerait pas sans la donnée, et particulièrement celle du consommateur. D'après Bruce Weinberg, il est légitime de s'interroger sur l'utilisation des données personnelles dans l'environnement web, mais elle en est d'autant plus préoccupante dans le domaine physique où les objets connectés permettent aux organisations, machines et programmes de prendre des décisions en fonction de caractéristiques propres au physique de l'Homme (battements de cœur, taux de sucre dans le sens, régime alimentaire, etc.).

L'Internet des objets permet de capturer la quasi-totalité des données relatives au comportement humain dans le monde physique. La hausse de la collecte des données, de leur traitement et de leur potentielle redistribution soulevait déjà quatre challenges éthiques pour Mason en 1986 :

- Le respect de la vie privée : quelles informations les individus transmettent à propos d'eux ou à propos d'autre groupes d'individus, sous quelles conditions, sont-ils forcés de révéler des informations les concernant ?
- La précision et la véracité : qui est responsable de la précision des informations collectées et de leur véracité ? Quel serait l'impact d'erreurs dans ces données pour des tiers ?
- La propriété : qui est propriétaire de la donnée, quelle est sa valeur ? À qui appartient le canal informationnel ?
- L'accessibilité : fait référence au droit des individus et des organisations à avoir accès aux informations collectées les concernant. Dans quelles démarches doivent-ils s'investir pour obtenir ces informations, qui les détiennent ?

De ces quatre challenges, Smith et al. (2011) font ressortir que le respect de la vie privée est celui qui préoccupe le plus les individus aujourd'hui dans un monde devenant de plus en plus connecté. D'après un rapport de la commission européenne, les entreprises

considèrent que les législations européennes concernant les données personnelles sont suffisantes, alors que les citoyens eux aimeraient que l'on y accorde une plus grande attention (Weber, 2015).

Le respect de la vie privée est au cœur de l'expérience utilisateur : avant d'adopter une technologie de l'Internet des objets, les consommateurs se prêtent à un rapport entre bénéfices et inconvénients apportés par la technologie.

Comme pour l'environnement web, plusieurs limites sont soulevées quant au respect de la vie privée dans le cadre de l'utilisation d'objets connectés. Xavier Caron et al. en soulèvent quatre principaux dans leur article de recherche *« The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective* » : une surveillance permanente dont les individus n'ont plus conscience, un manque de contrôle quant à la création et l'utilisation des données, des méthodes d'authentification non adaptées avec un manque d'anonymat, et de potentiels risques associés à la sécurité des informations collectées.

(1) Une surveillance permanente

La collecte de données personnelles dans le monde physique est permanente, les individus n'en ont plus conscience. Les capteurs et diverses applications permettent de collecter de nombreuses données sur les comportements et habitudes des individus et ce sans que ces derniers ne s'en rendent compte. Certains auteurs considéraient dans le début des années 2000 que cette collecte de données à l'insu des individus pouvait être considérée comme une forme « d'espionnage » et d'atteinte à la vie privée (Abowd et al., 2000). Cette collecte de données associée à des techniques de prédiction (data mining) exacerbe cette surveillance car les entreprises sont capables de prédire les comportements des individus. Xavier Caron et al. soulignent que près d'une vingtaine d'auteurs attestent qu'une partielle perte de vie privée est inévitable dans un contexte d'Internet des objets. La collecte d'une vaste quantité de données dans le but d'apporter de la valeur au consommateur est le principe même de l'environnement de l'Internet actuel (Lee et Lee, 2015). Les individus sont prêts à divulguer des données personnelles s'ils font confiance à l'organisation et s'ils obtiennent un bénéfice en retour. (Culnan et Armstrong, 1999). D'après une étude menée

par TRUSTe[4] aux États-Unis, seul 22% des internautes pensent que les bénéfices apportés par les objets connectés surpassent tout questionnement relatif à la vie privée ; 83% sont inquiets de cette constante collecte.

(2) Un manque de contrôle quant à la création et l'utilisation des données

Dans l'environnement de l'Internet des objets, les données sont créées en permanence. Les données sont générées automatiquement et ont besoin d'être stockées. L'architecture actuelle des data center n'est pas prête à accueillir un tel volume et une telle variété de données (Gartner, 2014). Cependant, outre le fait que les organisations soient à même de contrôler cette création de flux de données, la principale préoccupation pour de nombreux auteurs vient du fait que les organisations pourraient partager ces informations. Plus que la collecte elle-même, c'est donc le processus de diffusion des données collectées qui doit être contrôlé car il peut être préjudiciable aux individus (Weber, 2010). Cependant, dans un environnement de l'Internet où l'environnement web et celui de l'Internet des objets se confondent, le contrôle des informations collectées et échangées devient presque impossible (Atzori et al. 2010). Ainsi, si nous reprenons notre exemple du thermostat Nest, il serait possible pour Google de définir selon le réglage d'un thermostat et de la température extérieure, la localisation idéale du prochain lieu de vacances d'un consommateur en fonction de ses préférences « thermiques ». L'entreprise pourrait ainsi revendre ces informations sur des places de marchés publicitaires en ligne, où des agences de voyage seraient prêtes à payer enchérir pour toucher le bon consommateur.

Aujourd'hui, c'est l'État qui est responsable de la législation en vigueur sur son territoire concernant la collecte et les échanges de données. Il peut ainsi mettre en place des réglementations concernant des interdictions d'utilisation de certains produits ou services, des obligations vis-à-vis des consommateurs et des autorisations ou non de divulgation d'informations à des tiers (Weber, 2010). Pour Oriwoh et al., la gestion de la donnée dans l'environnement de l'Internet des objets inclut trois différents acteurs que sont les propriétaires (responsables du service proposé et du partage à des tiers), les fabricants de

[4] TRUSTe est une organisation proposant des services de conseils en termes de vie privée et propose des certifications relatives.

capteurs (responsables en cas de malfaçon ou de disfonctionnement) et les lois, les gouvernements (responsables de la protection des concitoyens).

En 2014, Hewlett Packard a analysé les capacités du top 10 des montres intelligentes sur le marché. Dans son rapport, l'organisation soulève que les données collectées sont souvent envoyées à plusieurs destinations, incluant des serveurs de tiers.

D'après l'étude de TRUSTe, 85% des internautes aimeraient mieux comprendre comment leurs données sont collectées et utilisées ; 88% d'entre eux aimeraient avoir un plus grand contrôle sur la collecte. Les nouvelles technologies de collecte et de traitement de la donnée couplées à un environnement législatif qui peine à s'actualiser, soulèvent des questions d'éthique. Quelles actions sont considérées comme étant « justes » ? Organisations et consommateurs pourraient avoir un point de vue différent sur ce questionnement éthique (Chessel, 2014). La position idéale se trouverait entre ce qui peut être fait techniquement, ce que l'organisation souhaite faire et ce qui est légal (voir figure n°6).

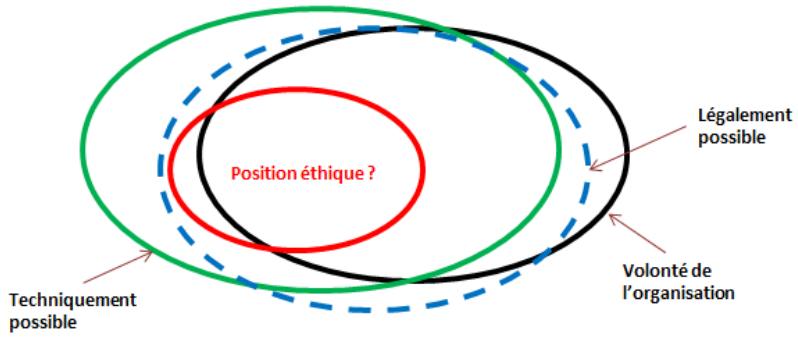


Figure n° 6 : Quel traitement éthique pour la donnée ? (Adaptation Chessel, 2014)

(3) Des méthodes d'identification non adaptées et un manque d'anonymat

Les méthodes d'identification lors de l'utilisation de services sont identiques et centralisées. Les individus s'identifient en utilisant leurs sessions Facebook, Google ou Apple avec un identifiant et un mot de passe, qui reste une méthode d'identification peu sécurisée. Les individus apprécient ce type de connexions qui sont simples et rapides mais ne sont peut-être pas conscients du fait qu'un hacking de l'un de ces comptes permettrait l'accès aux données de tous leurs objets connectés. D'après l'étude menée par Hewlett Packard, 80 % des objets connectés (incluant leur interface cloud et application mobile) présentaient des

méthodes d'authentification pauvres en termes de sécurité avec des mots de passe trop simples et ou trop courts de type « 1234 ».

Des risques liés à l'identification automatique d'individus entre des capteurs ou services de manière automatique peuvent être soulevés (Oriwoh et al, 2013). Les méthodes d'identification liées aux futures technologies doivent prendre en compte des systèmes d'authentification en accord avec les potentiels risques impliqués. L'anonymisation de la donnée se base sur des principes du cryptage comme :

- L'intraçabilité : deux informations ou deux actions issues d'un même utilisateur ne peuvent être mise en relation
- L'indétectabilité : un attaquant ne peut pas distinguer l'existence d'une information ou non
- L'inobservabilité : impossibilité de détecter si une application est utilisée par un utilisateur donné
- La confidentialité : le contenu des communications est confidentiel

Si les individus font confiance à la manière dont est faite l'identification avant l'utilisation du service, cela impliquera une confiance accrue dans la technologie de l'Internet des objets. L'utilisation de pseudonymes pour préserver l'anonymat des individus semble complexe à mettre en place dans cet environnement. Comme pour l'empreinte numérique, la quantité d'informations collectées dans de multiples situations permettrait de recréer des profils personnels d'individus (Beresfort et Stajano, 2003). Une étude démontre que sur une base de données anonymisée où la position d'individus est enregistrée toutes les heures avec la précision d'une antenne relais, quatre points spatio-temporels sont suffisants pour identifier de manière unique 95% des individus (De Montjoye et al, 2013). Dans un contexte de partages de données, des méthodes permettant de réellement garantir l'anonymat des individus, comme l'encryptage des données, doivent être développées.

Les différents niveaux de protections des données personnelles entre pays entrainent également des questionnements en termes de vie privée. C'est pourquoi, cette problématique doit rester centrale dans les débats concernant l'Internet des objets (Weber, 2015)

(4) Les risques de sécurité

La sécurité des informations collectées est également une préoccupation des individus, liée à la sécurité globale lors de l'utilisation d'une technologie de l'Internet des objets. Selon une étude La Poste Solution Business, 75% des Français pensent que la sécurité de leurs données personnelles est un frein à l'usage des objets connectés. Malgré cela, le nombre d'objets connectés par foyer s'accroit d'années en années. Ces objets du quotidien deviennent de potentielles cibles pour des attaques car ils collectent des informations personnelles concernant les individus (Vermesan et al., 2011). Ce risque de sécurité est exacerbé du fait qu'un nombre important de données collectées par des capteurs sont transmises à d'autres (Chen, 2012). Certains de ces capteurs ne peuvent offrir des protocoles de sécurité adéquats du fait de leur taille et de leur puissance de traitement (Chen, 2012). Ces capteurs sont susceptibles d'être victimes d'attaques du type *« man-in-the-middle »*, ce qui signifie qu'un tiers s'interpose secrètement entre deux parties qui pensent communiquer directement entre elles pour ainsi voler ou déformer des informations (Atzori et al. 2010). Pour de nombreux objets connectés, le cryptage et l'anonymisation des données ne se fait qu'à leur arrivée sur le cloud (Weber, 2015). Des méthodes de cryptage avancées doivent être utilisées par les organisations pour assurer la sécurité de l'information : confidentialité, intégrité et authenticité (Campbell et al. 2003), et ce, à tous les niveaux de son traitement, de la collecte à l'analyse.

En 2014, Hewlett Packard révélait que 70% des objets connectés les plus utilisés présentaient de sérieuses vulnérabilités comme l'absence d'encodage lors du transport des données, des interfaces web non sécurisées ou encore des vulnérabilités au niveau logiciel. En moyenne, chaque objet comportait 25 vulnérabilités et était sujet à attaques.

C. Objets connectés et avenir de la collecte de données : la transparence pour la confiance – Disney

La Commission Européenne pour la protection des données et la vie privée a approuvé la conclusion de la conférence africaine sur l'Internet des objets ayant eu lieu en 2014 à l'Île Maurice : « la transparence est la clé : ceux qui proposent des services relatifs à l'Internet des objets doivent être clairs sur les données qui sont collectées, pourquoi elles le sont et

combien de temps elles vont être stockées. ». Dans leur article paru dans la Harvard Business Review en mai 2015, Thimothy Morey et al. décrivent le paradoxe actuel de la collecte de données. Les consommateurs sont de plus en plus soucieux du fait que leurs données sont collectées, utilisées, analysées et revendues mais n'ont cependant pas conscience de ce qu'ils divulguent lorsqu'ils ont accès à l'Internet (environnement web et objets connectés confondus). La majorité des entreprises choisissent de ne pas divulguer de façon explicite ces pratiques ce qui porte préjudice à la confiance des consommateurs et à leur volonté de partager ces informations aux organisations. Aujourd'hui, c'est huit Français sur dix (81%) qui craignent que les données collectées par leurs objets connectés soient utilisées à des fins marketing (Intel, 2016)

La solution pour regagner cette confiance des consommateurs serait alors de développer des produits et services transparents quant au traitement des données et au respect de la vie privée. La valeur délivrée par les produits et services doit être proportionnelle à la valeur des données transmises par les individus, ces derniers doivent savoir comment les données sont collectées et pouvoir contrôler la transmission.

Les business models basés sur le traitement de la donnée personnelle impliquent de grandes responsabilités et par conséquent, l'établissement de règles strictes concernant les politiques de confidentialité et de traitement. Les entreprises devraient cependant prendre l'initiative de communiquer aux consommateurs leurs pratiques de tracking et leur finalité. Pour Timothy et al., le simple fait d'informer les individus d'un quelconque traitement de données par le biais de conditions d'utilisation n'est plus suffisant.

L'entreprise Disney est citée dans cet article pour avoir mis en pratique une approche client basée sur la confiance en mettant ses pratiques en lumière, en donnant aux clients le contrôle de leurs données et en délivrant de la valeur. En effet, Disney a investi plus d'un milliard de dollars dans le Magic Band, un bracelet connecté conçu pour optimiser les visites de leur parc d'Orlando.

Un bracelet connecté est envoyé au domicile des individus avant leur visite dans le parc. La boîte contenant le ou les bracelets contient une note d'information concernant l'objet connecté, son utilité, sa finalité et les méthodes de traitement des données qu'il collectera.

Ce dernier permet de paramétrer différentes variables comme par exemple les attractions préférées, le numéro de réservation de la chambre d'hôtel et le numéro de carte bancaire. Une fois le bracelet paramétré, les individus peuvent se rendre au parc et déverrouiller leur chambre d'hôtel grâce au bracelet, payer leurs achats dans les différents points de vente (magasins, restaurants, etc.) et bénéficier d'un parcours personnalisé dans le parc pour éviter les files d'attente. Les employés du parc disposent d'un terminal permettant de savoir où se trouvent les visiteurs mais également de connaître leur nom, ce qui permet de les accueillir nominativement lors de leur arrivée.

Les données collectées ont en somme permis d'améliorer l'expérience consommateur en s'appuyant sur l'analyse numérique, augmenté l'efficience opérationnelle grâce à une approche basée sur les données, permis l'interactivité entre les différents acteurs du parc grâce au digital (clients, employés, attractions, etc.) et également la personnalisation des objets connectés. Le bracelet a été conçu pour anticiper les désirs des consommateurs et ainsi rendre les visites du parc plus agréables, générer des revenus supplémentaires et fidéliser sa clientèle.

D. TAM - IOT dans le domaine de la santé

En novembre 2015, le web était utilisé par 87,9% de la population d'Amérique du Nord, 73,5% de la population Européenne, 40,2% de la population Asiatique et 46,4% de la population mondiale. Entre 2000 et 2015, le taux de pénétration de l'Internet au niveau mondial a été de 832,5% (Internet World Stats, 2015). L'environnement web est nécessaire au fonctionnement de nombreuses entreprises et sociétés, il a été largement adopté dans les pays développés. Cependant, comme nous l'avons vu précédemment, la collecte de données personnelles inquiète les consommateurs et les objets connectés apparaissent comme la technologie représentant l'avènement de la collecte d'informations sur les consommateurs.

Malgré les inquiétudes, les objets connectés étaient adoptés par un quart des Français en 2014 selon l'institut d'étude de marché et d'opinons BVA[5]. Dans ce même panel, 84% des Français considéraient le développement des objets connectés comme un progrès, et 6

[5] BVA est le 3ème institut d'études en France et présent dans le top 25 mondial

interrogés sur 10 plébiscitaient l'usage des objets connectés dans le domaine de la santé (BVA - Syntec numérique, 2014). Selon Gartner, les domaines spécialisés où l'adoption sera la plus large seront la fabrication (15%), la santé (15%) et l'assurance (11%) (Gartner, 2016).

Si les études semblent attester que les Français sont prêts à adopter les objets connectés, il n'en reste pas néanmoins que ces derniers peuvent être considérés comme intrusifs. De ce fait, sur quels leviers les entreprises devront-elles s'appuyer pour faciliter l'adoption de leurs technologies auprès des populations ?

Pour cette étude, nous allons prendre le cas de l'entreprise Google X, filiale d'Alphabet (anciennement Google) fondée en 2010. L'entreprise avait déjà commencé à développer en 2013 un prototype de nanoparticules permettant la détection de maladie incurables. La technologie devrait se présenter sous la forme d'une pilule à ingérer. Une fois dans l'estomac, des nanoparticules (2000 fois plus petites qu'une cellule sanguine) seraient libérées dans l'organisme et s'attacheraient aux cellules. Elles seraient ensuite capables de détecter des changements d'états annonciateurs de tumeurs, de crises cardiaques ou encore d'arrêts vasculaires cérébraux. Les nanoparticules pourraient alerter l'individu par le biais d'objets connectés, comme une montre par exemple.

Ce projet fait partie des « Moon Shots » d'Alphabet, projets révolutionnaires, à l'instar des Google Glass ou de la Google Car. Le but de Google X est de transformer le domaine médical où les diagnostics sont aujourd'hui de type réactifs, à un environnement où les diagnostics seraient proactifs tout au long de la vie, pour empêcher les individus de tomber malade (Georges, Les Echos, 2014).

Le choix de Google X et de son comprimé permettant de détecter la maladie parait pertinent du fait que ce dernier pourrait apporter un important bénéfice aux individus tout en collectant des données très sensibles relatives à la santé.

97% des personnes interrogées par l'équipe de Thimothy Orey sont soucieuses du fait qu'une entreprise ou un gouvernement puisse mal interpréter des données collectées. S'il était possible de payer pour protéger des données relatives à des antécédents médicaux, nos voisins allemands seraient prêts à débourser près de 185 € contre moins de 50 € pour un profil sur les réseaux sociaux ou un historique de recherche sur le web.

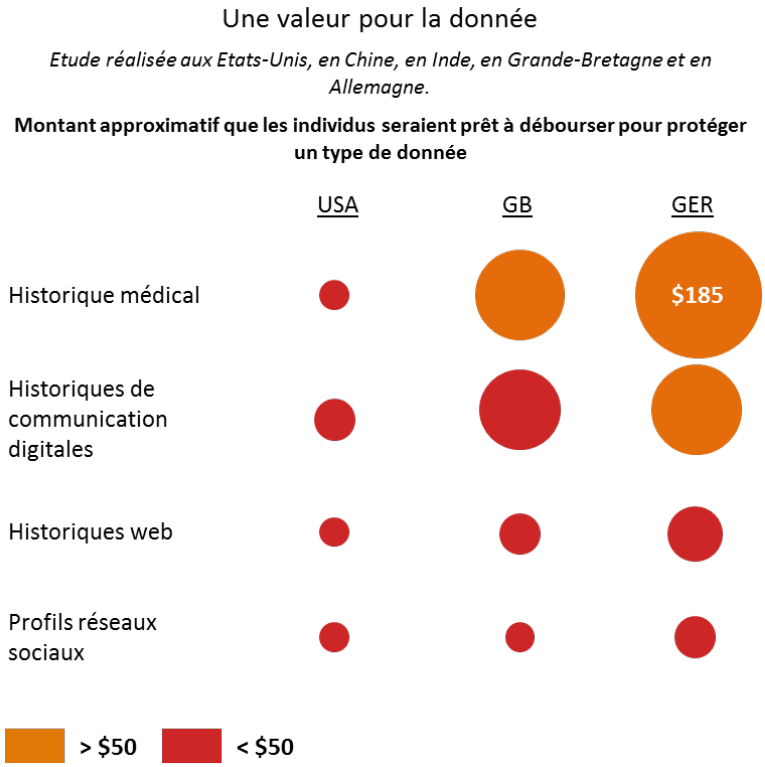


Figure n°7 : Une valeur pour la donnée (Morey, 2015)

Pour tenter de comprendre sur quelles variables les entreprises doivent s'appuyer pour convaincre leurs consommateurs d'utiliser leurs technologies, nous allons utiliser un modèle étendu du TAM (Technology of Acceptance Model) qui sera présenté ultérieurement et qui est inspiré du modèle utilisé par Vincent Dutot dans son article : *Factors influencing Near Field Communication (NFC) adoption: An extended TAM approach (2015)*. Avant d'adapter ce modèle à la technologie de Google, nous allons nous intéresser à ses origines.

1. Technology Acceptance Model

De nombreuses recherches ont mené des chercheurs à établir des modèles dans le domaine des systèmes d'informations pour comprendre quels facteurs pourraient influencer les individus à accepter une technologie. Des modèles sont spécialisés dans le domaine comportemental relatif à l'intention comme le TRA (Theory of Reasoned Action, Fishbein et Ajzen, 1975) ou le TPB (Theory of Planned Behavior, Ajzen, 1991). D'autres modèles comme le TAM ou l'UTAUT (Unified Theory of Acceptance and Use of Technology, Venkatesh, Morris, Davis, et Davis, 2003) sont quant à eux spécialisés dans le domaine de l'acceptation de la technologie. Le TAM a initialement été développé par Davis en 1989 et est encore à l'heure actuelle l'un des modèles les plus utilisés pour expliquer l'acceptation d'une

technologie par un individu et en déduire l'intention d'utilisation (Tan, Sim, Ooi, et Phusavat, 2012).

Le TAM se compose de deux principales variables que sont la simplicité d'utilisation perçue (*« perceived ease of use »)* et l'utilité perçue (*« perceived usefulness »)* qui se rapportent à l'intention d'utiliser la technologie. L'utilité perçue fait référence à la compréhension de l'individu des bénéfices et des améliorations sur son quotidien découlant directement de l'utilisation de la technologie. La simplicité d'utilisation perçue se réfère au degré d'investissement personnel que pense devoir donner l'individu pour utiliser une technologie. La simplicité du TAM l'a rendu très populaire au sein de la population scientifique. Néanmoins, pour améliorer son potentiel de prédiction, il est nécessaire de lui ajouter des variables externes supplémentaires (Davis, 1989 ; Rupanjali et al., 2013).

Dans les années 2000, Venkatesh et Davis ont développé le TAM 2 dans lequel des critères subjectifs ont été ajoutés comme l'image de la technologie du point de vue de l'individu, l'importance de son emploi ou encore son expérience. Venkatesh et al. introduisaient également en 2003 des concepts comme l'influence sociale, le genre, l'âge et les attentes en termes d'efforts pour l'adoption d'une technologie de l'information. Ces modifications apportées au TAM initial de Davis nous montrent qu'il est possible et intéressant d'adapter les modèles à la technologie étudiée.

Nous utiliserons donc le TAM en y ajoutant des variables externes en plus de l'influence sociale utilisée dans le modèle UTAUT (Venkatesh et al, 2003) qui a un poids important dans l'acceptation d'une technologie par un individu. L'influence sociale fait référence au poids du pouvoir de persuasion ou de l'opinion d'un entourage, pouvant conduire ou non à l'adoption d'une nouvelle technologie. L'influence sociale est un facteur subjectif qui se construit après des échanges d'opinions avec des personnes importantes pour l'individu (sa famille, ses amis) par rapport à une technologie (Fishbein et Ajzen, 1975). Le comportement de l'individu pourrait ainsi changer uniquement sous l'influence de ces personnes, même si leurs opinions divergent : c'est ce que l'on appelle la dissonance cognitive (Festinger, 1962).

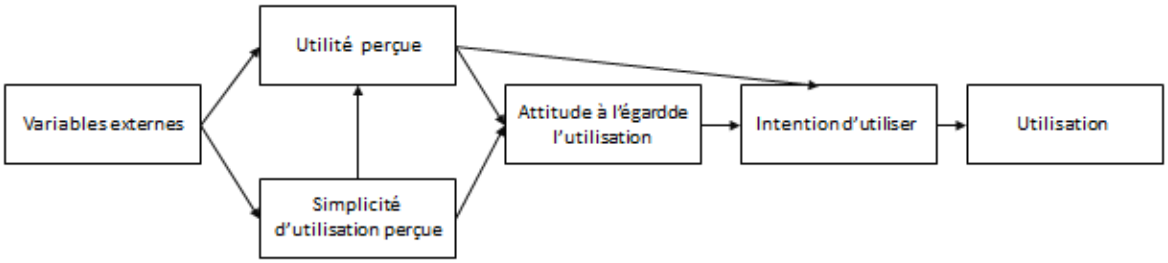


Figure n°8 : TAM (Davis, 1989)

2. TAM dans le contexte des objets connectés

Comme vu précédemment, les individus sont de plus en plus soucieux quant à la collecte de leurs données personnelles. Deux principaux points ont été mis en avant quant à leurs craintes : ils ne font pas pleinement confiance aux entreprises et ils doutent quant à la sécurité de leurs données. La technologie n'étant pas encore disponible à la vente, nous ajouterons un troisième point qui est le côté innovateur de l'individu. Étudions ces trois variables complémentaires à l'influence sociale.

(1) La confiance

La confiance est un facteur crucial dans l'environnement digital (Liu et al, 2004) et a été une pierre angulaire lors du développement du e-commerce et des réseaux sociaux (Dutot, 2014). Outre le monde digital, la confiance a toujours été au cœur des relations de long terme entre entreprises et consommateurs (Doney et Cannon, 1997).

La confiance est définie de nombreuses manières. Certaines recherches l'expliquent comme étant la bienveillance, l'intégrité ou encore l'empathie des relations entre entreprises et consommateurs (Flavian et al 2006). Pour d'autres, la confiance doit être considérée comme une composante du comportement, celui d'un individu vis-à-vis d'un autre et qui reflète le sentiment de sécurité qu'ont les parties entre elles (Md Nor et al, 2011). De ce point de vue, la confiance est traduite par la « volonté de dépendre » d'un tiers. D'autres recherches ont montré que si le consommateur ressent que l'entreprise est compétente, la confiance en sera positivement impactée. La confiance est aussi associée à de nombreuses sources de croyances (Doney et Cannon, 1997). Ce sentiment de confiance et la perception de

compétence sont très importants dans le domaine des technologies liées à la santé. Il est légitime pour le consommateur de se demander ce que vont devenir toutes les données collectées à son égard, et si ces dernières vont être partagées ou revendues à des tiers.

(2) La sécurité

En adoptant des technologies liées aux objets connectés, ici des nanotechnologies permettant la collecte de données relatives à la santé des individus, ces derniers s'exposent à des risques comme des malfaçons, des bugs, ou des attaques de hackers. Les consommateurs sont soucieux vis-à-vis des menaces de l'Internet.

La sécurité est relative à deux concepts : celui de la sécurité perçue et celui de respect de la vie privée (Radomir et Nistor, 2013). Il a été démontré que les deux concepts sont fortement liés et souvent traités ensemble (Nasri et Charfeddine, 2012). Malgré l'absence de contact humain direct dans la relation, la sécurité perçue et le respect de la vie privée sont des facteurs influençant l'adoption de services en ligne (Radomir et Nistor, 2013). La majorité des recherches faisant état de l'influence d'un facteur relatif à la sécurité ont été réalisées dans des environnements digitaux. Dans le secteur bancaire en ligne, si les individus ressentent que leurs transactions sont réalisées de manière sécurisée et que leurs informations personnelles restent privées, cela influencera positivement leur décision d'accepter ce type de technologies (Wang et al, 2003).

(3) Côté innovateur de l'individu

Certains individus adoptent rapidement les nouvelles technologies alors que d'autres les rejettent. De cette observation, plusieurs recherches ont eu lieu notamment avec Rogers en 1983 qui conceptualisait le modèle comportemental et social des individus au moment d'adopter une nouvelle technologie. Le côté innovateur d'un individu impacte positivement l'intention d'adoption d'une innovation. Les recherches ont démontré qu'il est important de distinguer l'innovation d'un point de vue « global » et d'un point de vue « spécifique », appliqué à un domaine en particulier (Flynn et Goldsmith, 1993). Michael Kirton prouvait également dans ses travaux que par nature, certains individus s'adaptent alors que d'autres innovent. Le côté innovateur de l'individu est un trait de personnalité propre à tout un chacun, à un plus ou moins fort degré (Kirton 1976). En se basant sur de précédentes recherches, Ritu Agarwal et Jayesh Prasad définissent alors le côté innovateur de l'individu

dans le domaine des technologies de l'information comme étant la volonté d'un individu d'essayer toute nouvelle technologie (Agarwal et Prasad, 1998).

3. Modèle de recherche et hypothèses

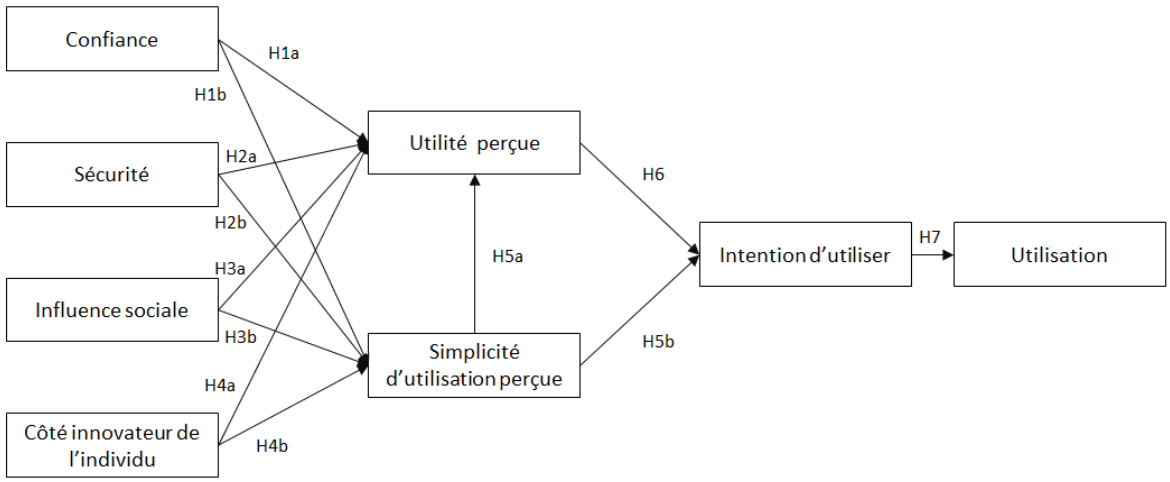


Figure n°9 : Modèle de recherche - TAM étendu

La relation positive entre la confiance et l'utilité perçue a été démontrée dans des recherches précédentes (Gefen et al, 2003). Pour Eriksson, Kerem et Nilsson, la confiance a un impact positif sur l'utilité perçue et la simplicité d'utilisation perçue. Voici nos hypothèses :

H1a : Il y a une relation significative entre la confiance et l'utilité perçue d'un individu vis-à-vis de l'objet connecté de Google

H1b : Il y a une relation significative entre la confiance et la simplicité d'utilisation perçue d'un individu vis-à-vis de l'objet connecté de Google

De précédentes recherchent ont démontré que les individus ont besoin d'être convaincus sur l'aspect sécuritaire d'une technologie avant de l'adopter (Yousafzai, Pallister, et Foxall, 2003). Dutot a démontré en 2015 que la sécurité a un impact sur la simplicité d'utilisation perçue. D'un autre côté, certains auteurs démontrent que la sécurité n'a pas de relation significative sur la simplicité d'utilisation perçue et l'utilité perçue (Chen et al, 2009).

H2a : Il y a une relation significative entre la sécurité et l'utilité perçue d'un individu vis-à-vis de l'objet connecté de Google

H2b : Il y a une relation significative entre la sécurité et la simplicité d'utilisation perçue d'un individu vis-à-vis de l'objet connecté de Google

L'influence sociale affecte l'utilisation de nouvelles technologies (Rupanjali et al, 2013). Taylor et Todd ont observé en 1995 le rôle que jouaient les opinions des individus, des proches et des supérieurs hiérarchiques sur l'influence sociale.

H3a : Il y a une relation significative entre l'influence sociale et l'utilité perçue d'un individu vis-à-vis de l'objet connecté de Google

H3b : Il y a une relation significative entre l'influence sociale et la simplicité d'utilisation perçue d'un individu vis-à-vis de l'objet connecté de Google

Le côté innovateur de l'individu dans le domaine des nouvelles technologies impacte l'intention d'utilisation (Agarwal et Prasad, 1998). Nous allons rechercher une relation avec l'utilité perçue et la simplicité d'utilisation perçue.

H4a : Il y a une relation significative entre le côté innovateur d'un individu et l'utilité perçue d'un individu vis-à-vis de l'objet connecté de Google

H4b : Il y a une relation significative entre le côté innovateur d'un individu et la simplicité d'utilisation perçue de l'individu vis-à-vis de l'objet connecté de Google

Les variables de la simplicité d'utilisation perçue et de l'utilité perçue du TAM influencent l'intention d'utilisation. Le TAM est encore aujourd'hui l'un des modèles les plus utilisés parmi les chercheurs en technologie de l'information (Venkatesch et al, 2003). La simplicité d'utilisation et l'utilité perçue font partie des cinq échelles de marketing les plus utilisées dans les recherches (Jeyaraj, Rottman, et Lacity, 2006). De ce fait, nous pouvons établir les hypothèses suivantes :

H5a : La simplicité d'utilisation perçue a un impact positif sur l'utilité perçue de l'objet connecté de Google

H5b : La simplicité d'utilisation perçue a un impact positif sur l'intention d'utilisation de l'objet connecté de Google

H6 : L'utilité perçue a un impact positif sur l'intention d'utilisation de l'objet connecté de Google

H7 : L'intention d'utilisation a un impact positif sur l'utilisation effective de l'objet connecté de Google

III. Méthodologie

A. Construction du questionnaire

1. Les échelles de mesure

Le questionnaire a été élaboré en s'inspirant du modèle du TAM de Davis et de la recherche effectuée par Vincent Dutot en 2015 sur les facteurs influençant l'adoption de la technologie NFC. La partie du questionnaire concernant directement le TAM a été divisée en six sections en fonction des différentes variables. En tout, le questionnaire comportait 36 questions (dont quatre concernant les caractéristiques démographiques, et une concernant le sentiment d'intrusivité de la technologie)).

Le questionnaire comportait huit construits relatifs au TAM pour mesurer l'acceptation d'un objet connecté relatif à la santé. Quatre questions se rapportaient à la confiance, basées sur les recherches de Liu et al. en 2004. La sécurité comportait trois questions, basées sur les recherches de Wang et al. en 2003. Le construit de l'influence sociale comportait trois questions et a été construit grâce aux travaux de Venkatesh et Davis en 2000 et de Taylor et Todd en 1995. Le côté innovateur de l'individu comportait quatre questions suite aux recherches d'Agarwal et Prasad en 1998. Pour les autres échelles, nous nous sommes inspirés des travaux initiaux de Davis (1989) (Simplicité d'utilisation, 5 questions – Utilité perçue, 6 questions – Intention d'utilisation, 3 questions – Utilisation, 3 questions).

Après avoir élaboré un premier questionnaire et à la suite de tests sur des proches et collègues, ce dernier a été modifié et amélioré pour faciliter la compréhension de certaines questions. À la suite de réactions de proches à la lecture du questionnaire, il a été décidé d'en réaliser un deuxième en changeant la technologie pour un bracelet apportant les mêmes bénéfices et limites perçues pour les individus. Nous avons ensuite comparé les deux panels pour vérifier que la forme de la technologie (pilule vs. bracelet) a un impact sur les répondants.

Echelle de mesure	Item	Question
Simplicité d'utilisation	SU1	Il sera simple pour moi d'apprendre à utiliser cette solution
	SU2	Utiliser cette solution demandera beaucoup d'effort intellectuel
	SU3	La façon d'utiliser cette solution me semble claire et compréhensible
	SU4	De façon générale, je trouve cette solution simple d'utilisation
	SU5	La solution présentée me semble compliquée à utiliser
Utilité perçue	UP1	Utiliser cette solution pourra améliorer ma qualité de vie
	UP2	Utiliser cette solution me donnera un plus grand contrôle sur ma santé
	UP3	Cette solution me fera gagner du temps car j'aurai moins besoin d'aller faire d'examens médicaux
	UP4	Utiliser cette solution me permettra de vivre plus longtemps
	UP5	Utiliser cette solution me rendra la vie plus facile
	UP6	De façon générale, je trouve cette solution utile dans mon quotidien
Intention d'utilisation	IU1	Je pense acheter cette solution lorsqu'elle sera disponible à la vente
	IU2	Je pense utiliser cette solution pour prévenir de potentielles maladies graves
	IU3	Je pense utiliser cette solution car elle peut m'être bénéfique
Influence sociale	IS1	Ma famille et/ou mes amis pourraient penser que je dois utiliser cette solution
	IS2	Des personnes importantes pour moi pourraient penser que je dois utiliser cette technologie
	IS3	Des supérieurs hiérarchiques pourraient penser que je dois utiliser cette solution
Utilisation	US1	Je me sens capable d'utiliser cette solution
	US2	Je considère que la décision d'utiliser cette solution ne dépend que de moi
	US3	Je pense avoir les compétences nécessaires pour utiliser cette solution
Sécurité	SE1	Je considère que cette solution peut présenter des risques en termes de sécurité
	SE2	Je considère qu'utiliser cette solution pour établir mon bilan médical n'est pas très sécurisé
	SE3	Je suis inquiet du fait que les informations collectées puissent être interceptées par des tiers
Confiance	CO1	Si les conditions d'utilisation de mes données me sont exposées, je ferai confiance à cette solution
	CO2	Si les conditions de partage de mes données avec des tiers me sont exposées, je ferai confiance à cette solution

	CO3	La possibilité d'accéder facilement aux informations collectées pour que je puisse les vérifier me donne le sentiment que la solution est digne de confiance
	CO4	Si l'entreprise m'expose les règles de confidentialité et de sécurité, je serai rassuré quant à l'utilisation de cette solution
Côté innovateur	CI1	En général, lorsque j'entends parler d'une innovation technologique, j'essaye de trouver un moyen de l'essayer
	CI2	Dans mon entourage, je suis généralement le premier à essayer les nouvelles technologies
	CI3	En général, je suis hésitant à l'idée d'essayer de nouvelles technologies
	CI4	J'aime essayer de nouvelles technologies

Tableau n°4 : Échelles de mesure

Toutes les variables ont été mesurées en utilisant des échelles de Lickert variant de 1 (pas du tout d'accord) à 5 (tout à fait d'accord).

2. Méthode de collecte des données

La période de collecte des données a durée approximativement 4 semaines. Les répondants étaient principalement des étudiants de l'Université de Strasbourg, des professeurs, collègues et proches. Aucune question filtre n'empêchait les individus de répondre, cependant, les personnes n'ayant pas la nationalité française ont été retirés de l'échantillon avant analyse (23 individus).

Pour l'élaboration du questionnaire et son administration, l'outil formulaire de Google a été utilisé (Google Form). Le lien renvoyant à ce dernier a ensuite été transmis sur des groupes Facebook et LinkedIn, via Twitter, ou encore par email.

En se basant sur le calculateur d'échantillon de Soper, le nombre de données collectées étaient suffisant pour les deux questionnaires avec un total de 471 répondants proportionnellement distribués (5 variables latentes et 31 variables à observer, intervalle de confiance de 95% et 5% de marge d'erreur tolérée, taille de l'échantillon minimum recommandé : 200).

3. Statistiques descriptives

Les répondants à l'étude sont majoritairement des étudiantes de moins de 45 ans (pour plus de 85% de la population). Toutes les données démographiques sont présentées dans le tableau ci-après.

	Caractéristique	Fréquence	%
Sexe	Homme	171	36,31%
	Femme	300	63,69%
Age	15-25	354	75,16%
	25-45	60	12,74%
	46-60	48	10,19%
	Plus de 60	9	1,91%
CSP	1-Agriculteurs exploitants	1	0,21%
	2-Artisans, commerçants et chefs d'entreprise	10	2,12%
	3-Cadres et professions intellectuelles supérieures	75	15,92%
	4-Professions intermédiaires	17	3,61%
	5-Employés	71	15,07%
	6-Ouvriers	3	0,64%
	7-Retraités	10	2,12%
	8-Autres personnes sans activité professionnelle	284	60,30%

Tableau n°5 : Statistiques descriptives

B. Résultats

1. Calculs

Premièrement, il convient de décider si les deux questionnaires peuvent être traités de façon commune ou si la différenciation de technologie a eu un impact sur les répondants.

En ce qui concerne le caractère intrusif de la technologie, les répondants considèrent en moyenne que le bracelet l'est à 5.74/10 contre 6.93/10 pour la pilule.

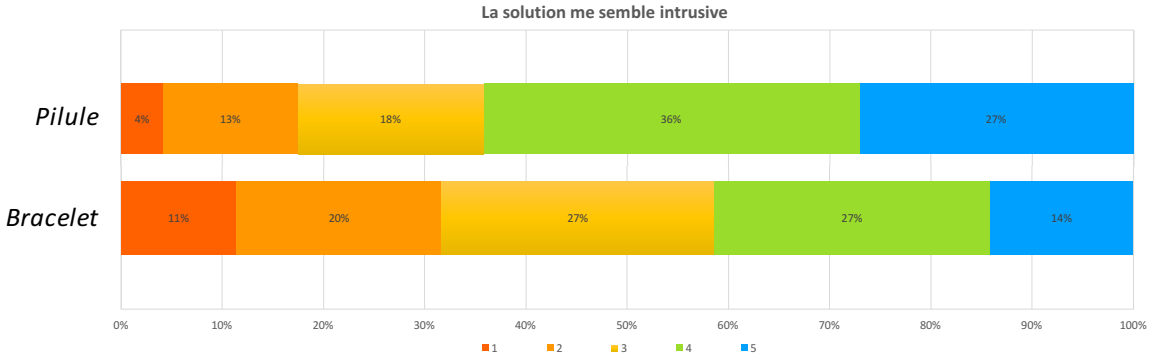


Figure n°10 : Sentiment d'intrusivité

D’après le test de Wilcoxon, la différence de ces moyennes est significative, ce qui signifie que les deux panels n’ont pas perçu les technologies de la même manière. Nous allons donc effectuer deux analyses : l’une pour la pilule, et l’autre pour le bracelet, pour ainsi analyser si les mêmes variables influencent l’adoption de ces technologies, et dans quelles mesures.

Nous pouvons déjà remarquer de manière visuelle que les deux panels n’ont pas répondu de la même manière en observant les statistiques univariées de certaines variables.

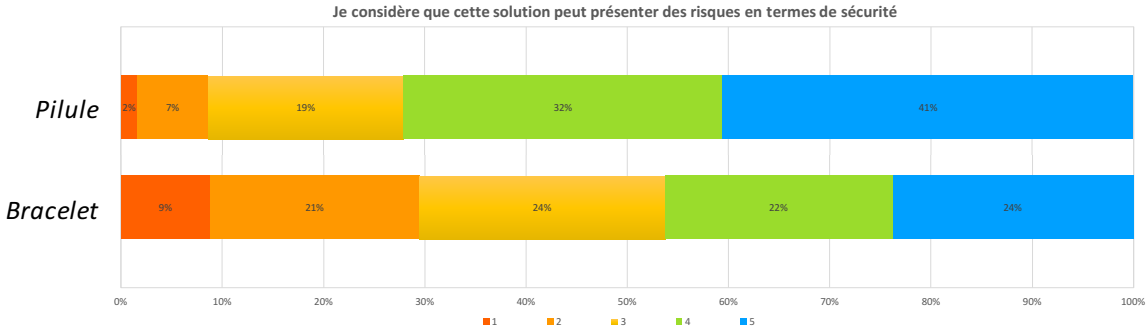


Figure n°11 : Sentiment de risques en termes de sécurité

De façon générale, 73% des répondants considèrent que la pilule présente des risques en termes de sécurité, contre 46% pour le bracelet.

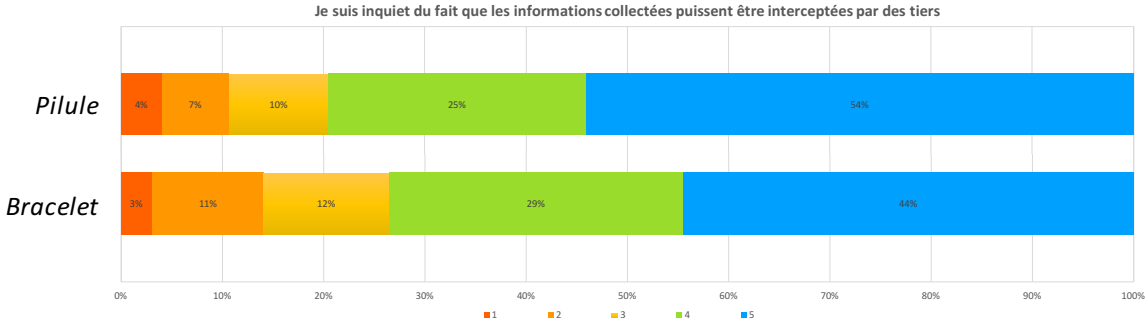


Figure n°12 : Sentiment de risques d’interception des données pour le bracelet

De façon générale, 79% des répondants sont inquiets du fait que leurs informations puissent être interceptées par des tiers à travers la pilule, contre 73% pour le bracelet.

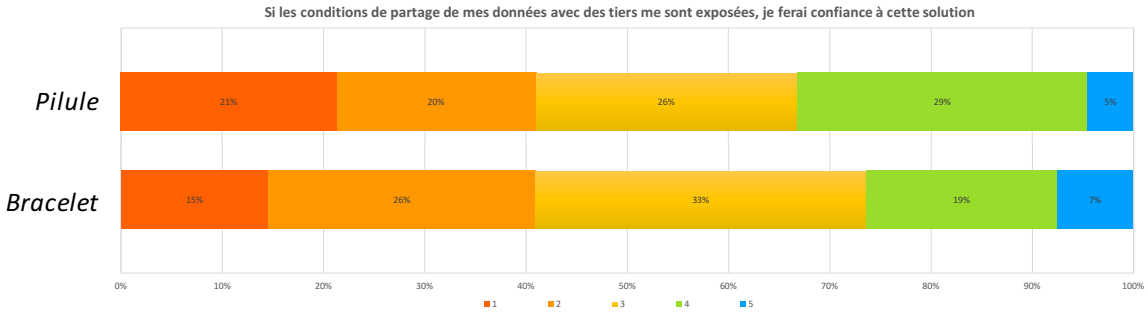


Figure n°13 : Sentiment de confiance suite à l'exposition des conditions de partage des données à des tiers

Même si les conditions de partage des données étaient exposées, 21% des individus n'auraient pas du tout de sentiment de confiance vis-à-vis de la pilule, contre 15% pour le bracelet.

Après avoir fait quelques comparaisons de statistiques univariées, nous allons procéder à des analyses indépendantes concernant les deux technologies. Toutes les autres statistiques univariées se trouvent en annexes.

a) Calculs pour la technologie : pilule

Premièrement, nous avons vérifié la validité des huit facteurs composant le modèle (simplicité d'utilisation, utilité perçue, intention d'utilisation, influence sociale, utilisation, sécurité, confiance et côté innovateur) grâce à une analyse factorielle. Cette analyse permet de mesurer la moyenne des variables et leur variance cumulée. Pour valider un facteur, les variables doivent se dessiner sur un seul axe avec une valeur minimum de 0.5 (Chen et Chang, 2013) et doivent posséder un alpha de Crombach qui dépasse 0.7, même si 0.6 est accepté dans un contexte de recherche (Hair et al, 2011). Les questions ne permettant pas aux facteurs de l'étude de se dessiner ont été retirées. Au final, nous retenons 3 facteurs pour la simplicité d'utilisation, 6 pour l'utilité perçue, 3 pour l'intention d'utilisation, 3 pour l'influence sociale, 1 pour l'utilisation, 3 pour la sécurité, 4 pour la confiance et 4 pour le côté innovateur. Le tableau ci-dessous illustre les résultats obtenus pour la pilule.

Facteur	Variable	Moyenne	Loading	Variance cumulée	Alpha de Crombach
Simplicité d'utilisation	SU3	3.967	0.658	0.548	0.736
	SU4	3.975	0.988		
	SU5	3.786	0.483		
Utilité perçue	UP1	3.397	0.759	0.552	0.879
	UP2	3.639	0.729		
	UP3	3.008	0.654		
	UP4	2.823	0.681		
	UP5	2.799	0.800		
	UP6	2.987	0.822		
Intention d'utilisation	IU1	2.118	0.863	0.771	0.909
	IU2	2.741	0.862		
	IU3	2.762	0.908		
Influence sociale	IS1	2.598	0.919	0.688	0.843
	IS2	2.692	0.949		
	IS3	2.381	0.566		
Utilisation	US3	4.323	0.997		
Sécurité	SE1	4.024	0.788	0.398	0.638
	SE2	3.750	0.599		
	SE3	4.188	0.462		
Confiance	CO1	3.008	0.910	0.665	0.887
	CO2	2.754	0.878		
	CO3	2.827	0.689		
	CO4	2.963	0.764		
Côté innovateur	CI1	2.954	0.707	0.550	0.828
	CI2	2.778	0.725		
	CI3	3.524	0.717		
	CI4	3.770	0.812		

Tableau n°6 : Analyse factorielle pour la pilule

À noter que pour mener l'étude à son terme, un seul facteur a été retenu pour l'utilisation. La cinquième question concernant la simplicité d'utilisation et la troisième question concernant la sécurité ont également été retenues pour les mêmes raisons, nonobstant que leurs valeurs sont inférieures à 0.5. Tous les autres facteurs et construits respectent les exigences citées ci-dessus.

Après avoir réalisé l'analyse factorielle, nous avons réalisé des régressions linéaires. Ces dernières nous permettent de voir les destinations d'influence des facteurs, dans quelles proportions ces derniers sont expliqués, et de valider nos hypothèses.

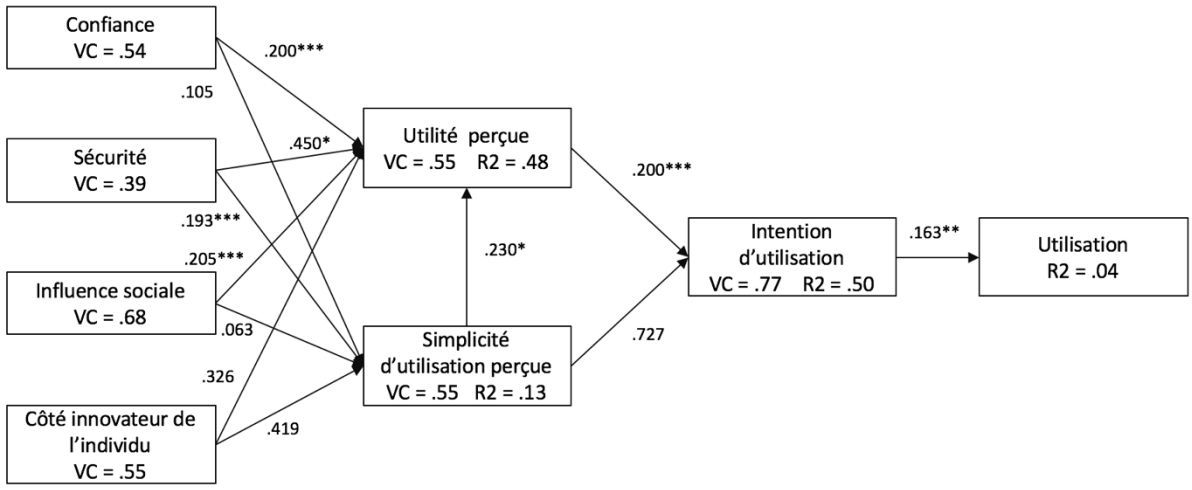


Figure n°15 : Résultats du TAM étendu pour la pilule

Au total, 7 hypothèses ont été validées : la confiance (CO), la sécurité (SE), l'influence sociale (IS) et la simplicité d'utilisation (SU) influencent l'utilité perçue (UP), la sécurité influence la simplicité d'utilisation perçue, l'utilité perçue influence l'intention d'utilisation (IU), et finalement, l'intention d'utilisation influence l'utilisation (US) effective de la technologie.

Relation entre les hypothèses	Significativité	T statistic	Validation
H1a : Confiance sur UP	0.200***	8.467	Accepté
H1b : Confiance sur SU	0.105	1.624	Rejeté
H2a : Sécurité sur UP	0.450*	-2.009	Accepté
H2b : Sécurité sur SU	0.193***	-3.787	Accepté
H3a : Influence sociale sur UP	0.205***	5.351	Accepté
H3b : Influence sociale sur SU	0.063	1.866	Rejeté
H4a : Côté innovateur sur UP	0.326	0.984	Rejeté
H4b : Côté innovateur sur SU	0.419	0.809	Rejeté
H5a : SU sur UP	0.230*	2.287	Accepté
H5b : SU sur IU	0.727	-0.350	Rejeté
H6 : UP sur IU	0.200***	14.939	Accepté
H7 : IU sur US	0.163**	3.187	Accepté

*p<0.05
**p<0.01
***p<0.001

Tableau n°7 : Validité des hypothèses pour la pilule

Après avoir accepté et rejeté les différentes hypothèses, il convient de définir quelles variables ont le plus d'impact sur l'utilité perçue et la simplicité d'utilisation des technologies. Pour cela, nous effectuons un calcul d'élasticité. L'élasticité de Y par rapport à X est la variation de Y en pourcentage due à une variation de X de 1%.

$$Elasticité\ de\ \Upsilon\ par\ rapport\ \text{à}\ \mathrm{X} = \Upsilon'_{\chi} \times \frac{\overline{\mathrm{X}}}{\overline{\overline{\Upsilon}}}$$

Nous pouvons ainsi voir que la variable « confiance » se détache particulièrement des autres en ce qui concerne l'utilité perçue de la technologie. Une variation de 1% du niveau de confiance entraîne une hausse de 0.39% de l'utilité perçue, toute chose étant égale par ailleurs. Les variables « sécurité » et « influence sociale » entraînent respectivement une variation 0.15% et 0.18%.

En ce qui concerne la simplicité d'utilisation, une variation positive de 1% du sentiment de sécurité entraîne une hausse de 0.22% de la variable.

Élasticité sur utilité perçue	**Dérivée**	**Moyenne**	**Elasticité (en %)**
Confiance	0.633	11.553	0.392
Influence sociale	0.440	7.672	0.181
Sécurité	-0.244	11.963	-0.156
Simplicité d'utilisation	0.254	10.156	0.138

Élasticité sur simplicité d'utilisation	**Dérivée**	**Moyenne**	**Elasticité (en %)**
Sécurité	-0.347	11.963	-0.223

Tableau n°8 : Élasticité des facteurs pour la pilule

b) Calculs pour la technologie : bracelet

Comme vu précédemment, les exigences concernant la méthode restent identiques, nous présentons ici les résultats.

Nous retenons 3 facteurs pour la simplicité d'utilisation, 6 pour l'utilité perçue, 3 pour l'intention d'utilisation, 3 pour l'influence sociale, 1 pour l'utilisation, 3 pour la sécurité, 4 pour la confiance et 4 pour le côté innovateur. Le tableau ci-dessous illustre les résultats obtenus pour le bracelet.

Facteur	Variable	Moyenne	Loading	Variance cumulée	Alpha de Conbach
Simplicité d'utilisation	SU1	4.105	0.550	0.591	0.785
	SU3	3.845	0.743		
	SU4	3.929	0.959		
Utilité perçue	UP1	3.493	0.822	0.520	0.859
	UP2	3.564	0.766		
	UP3	2.744	0.535		
	UP4	2.704	0.631		
	UP5	2.907	0.744		
	UP6	3.136	0.789		
Intention d'utilisation	IU1	2.299	0.808	0.753	0.899
	IU2	3.000	0.867		
	IU3	2.939	0.924		
Influence sociale	IS1	2.524	0.959	0.670	0.816
	IS2	2.568	0.935		
	IS3	2.163	0.472		
Utilisation	US3	4.400	0.997		
Sécurité	SE1	3.317	0.833	0.476	0.711
	SE2	3.550	0.681		
	SE3	4.008	0.519		
Confiance	CO1	3.105	0.864	0.667	0.888
	CO2	2.784	0.843		
	CO3	2.898	0.765		
	CO4	3.123	0.791		
Côté innovateur	CI1	2.819	0.747	0.529	0.810
	CI2	2.590	0.811		
	CI3	3.392	0.558		
	CI4	3.528	0.768		

Tableau n°9 : Analyse factorielle pour le bracelet

Comme pour la pilule, un seul facteur a été retenu pour l'utilisation. La troisième question concernant l'influence sociale a également été retenue, nonobstant que la valeur soit proche bien qu'inférieure à 0.5. Tous les autres facteurs et construits respectent les exigences pour réaliser les régressions linéaires.

Après avoir réalisé l'analyse factorielle, nous avons réalisé des régressions linéaires. Ces dernières nous permettent de voir les destinations d'influence des facteurs, dans quelles proportions ces derniers sont expliqués, et de valider nos hypothèses.

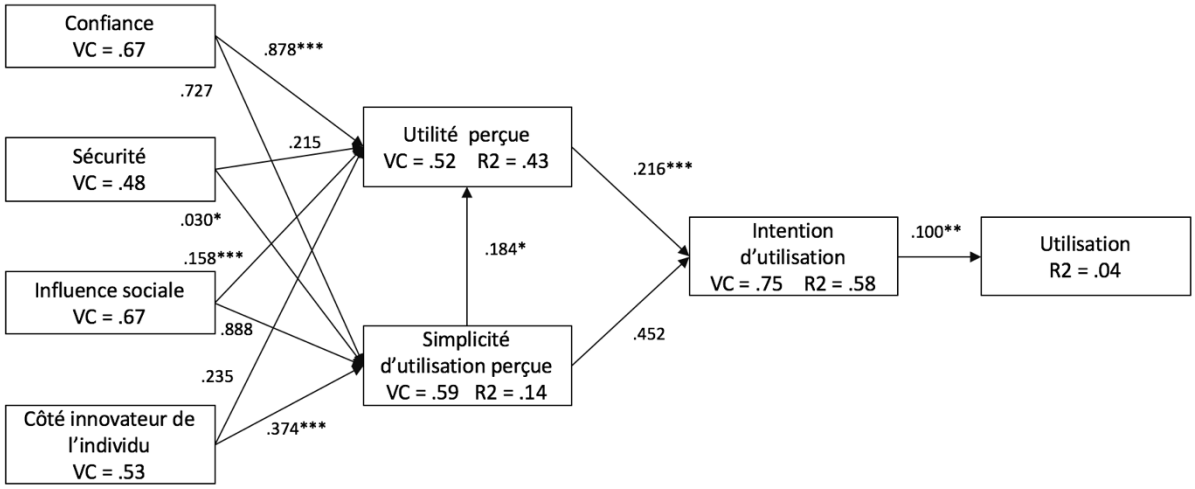


Figure n°16 : Résultats du TAM étendu pour le bracelet

Au total, et comme pour la pilule, 7 hypothèses ont été validées. Les facteurs influençant l'adoption ne sont cependant pas les mêmes : : la confiance (CO), la simplicité d'utilisation (SU) et l'influence sociale (IS) influencent l'utilité perçue (UP), la sécurité (SE) et le côté innovateur (CI) influencent la simplicité d'utilisation perçue, l'utilité perçue influence l'intention d'utilisation (IU), et finalement, l'intention d'utilisation influence l'utilisation (US) effective de la technologie.

Relation entre les hypothèses	Significativité	T statistic	Validation
H1a : Confiance sur UP	0.878***	7.592	Accepté
H1b : Confiance sur SU	0.727	0.349	Rejeté
H2a : Sécurité sur UP	0.215	-1.241	Rejeté
H2b : Sécurité sur SU	0.030*	-2.182	Accepté
H3a : Influence sociale sur UP	0.158***	5.417	Accepté
H3b : Influence sociale sur SU	0.888	-0.141	Rejeté
H4a : Côté innovateur sur UP	0.235	1.190	Rejeté
H4b : Côté innovateur sur SU	0.374***	4.745	Accepté
H5a : SU sur UP	0.184*	2.375	Accepté
H5b : SU sur IU	0.452	0.754	Rejeté
H6 : UP sur IU	0.216***	16.979	Accepté
H7 : IU sur US	0.100**	3.305	Accepté

*p<0.05
**p<0.01
***p<0.001

Tableau n°10 : Validité des hypothèses pour le bracelet

Suite aux calculs d'élasticité, nous pouvons voir que la variable « confiance » se détache particulièrement des autres en ce qui concerne l'utilité perçue de la technologie. Une variation de 1% du niveau de confiance entraîne une hausse de 0.38% de l'utilité perçue, toute chose étant égale par ailleurs. Les variables « simplicité d'utilisation » et « influence sociale » entraînent respectivement une variation 0.17% et 0.18%.

En ce qui concerne la simplicité d'utilisation, une variation positive de 1% du sentiment de sécurité entraîne une hausse de 0.20% de la variable. Une variation de 1% du côté innovateur de l'individu entraîne une hausse de 0.18%.

Élasticité sur utilité perçue	Dérivée	Moyenne	Elasticité (en %)
Confiance	0,592	11,912	0,380
Influence sociale	0,479	7,256	0,187
Simplicité d'utilisation	0,274	11,881	0,176

Élasticité sur simplicité d'utilisation	Dérivée	Moyenne	Elasticité (en %)
Côté Innovateur	0,144	13,029	0,185
Sécurité	-0,170	11,963	-0,201

Tableau n°11 : Élasticité des facteurs pour le bracelet

2. Analyses et recommandations

Il est ici démontré que la forme physique de l'objet connecté a un impact sur l'ensemble des variables et donc sur la manière dont la population perçoit les opportunités et les défis liés à la solution. Nous allons effectuer des recommandations suite à l'analyse des résultats.

Pour les deux technologies confondues, les quatre variables externes ont eu des impacts sur le modèle, mais de façon différente.

Pour la pilule, ce sont la confiance, la sécurité et l'influence sociale qui jouent un rôle primordial. Dans le secteur des technologies, la confiance du consommateur est cruciale pour les organisations et joue un rôle majeur dans l'adoption (Flavial et al, 2006). La confiance influence directement et de manière significative l'utilité perçue de la technologie pour les répondants. Les organisations doivent être transparentes quant à la collecte, l'utilisation et le partage des données qui leurs sont confiées par les consommateurs. Dans ce souci de transparence, Google a récemment notifié ses utilisateurs d'un changement dans ses règles de confidentialité concernant son moteur de recherche. L'entreprise a communiqué autour de ces modifications par le biais d'un formulaire interactif et illustré pour jouer sur un côté sympathique et proche de ses utilisateurs. Aussi, après sa conférence I/O et la présentation du nouvel assistant vocal de Google pour la maison, Google Home, Sundar Pichai[6] a affirmé que le produit disposera d'un mode Incognito. Les consommateurs sont inquiets par rapport à la collecte de leurs données personnelles et ont besoin d'être rassurés. Avec ces démarches, Google rassure et espère gagner la confiance de ses futurs consommateurs.

Le modèle montre que l'influence sociale est le deuxième facteur le plus significatif en ce qui concerne l'utilité perçue de l'objet connecté. Pour influencer cette variable, les organisations doivent communiquer par le biais d'influenceurs, des personnes de confiance, pour permettre aux consommateurs d'adopter la technologie. Le rôle crucial du bouches-à-oreilles avait également été démontré dans de précédentes recherches (Dutot, 2015 et Barreto, 2014) et nos résultats l'attestent de la même façon.

[6] Sundar Pichai est l'actuel PDG de Google

La sécurité influence l'utilité et la simplicité d'utilisation perçue de la technologie. Cela signifie que dans le but de faciliter l'adoption de leurs objets connectés, les entreprises doivent mettre l'accent sur la sécurité et l'encryptage des données. Le concept de sécurité et son rôle dans le TAM avait déjà été démontré (Dutot, 2015). Le fait de l'introduire dans le domaine des objets connectés de la santé et de démontrer son importance nous permet de renforcer le concept.

Il est intéressant de noter que dans le cas de la pilule, le côté innovateur de l'individu n'a aucun effet sur l'adoption. Pour expliquer ce phénomène, nous avons formulé deux hypothèses qui nous semblent pertinentes. La première est que dans le contexte du domaine de la santé, la pilule a été perçue comme un médicament, et non comme un objet connecté. Si la technologie n'a pas été perçue comme en étant une, le côté innovateur de l'individu n'a pu entrer en jeu. La deuxième hypothèse est le côté trop futuriste de cet objet connecté. Bien que Google X souhaite mettre cette solution sur le marché dans un futur proche, la technologie est peut-être encore trop éloignée du quotidien des individus.

Pour le bracelet, ce sont la confiance, la sécurité, l'influence sociale et le côté innovateur des individus qui jouent un rôle dans l'adoption de l'objet connecté. Ces variables ont la même définition mais ne sont pas significatives sur les mêmes facteurs. La confiance et l'influence sociale dans une moindre mesure, restent les influenceurs majeurs de l'utilité perçue.

En revanche, la sécurité ne joue plus de rôle dans cette relation. La sécurité influence désormais la simplicité d'utilisation. Cela signifie que plus les entreprises sécuriseront leurs objets connectés, leurs interfaces, et les données collectées par ce biais, plus les consommateurs seront enclins à utiliser les technologies. En ce qui concerne la pilule et le bracelet, la sécurité joue un rôle important dans le sens où les individus ne veulent pas que d'autres entreprises ou tiers puissent intercepter ces données personnelles sensibles.

Le côté innovateur de l'individu entre en jeu dans la relation et influence la simplicité d'utilisation perçue. Nous pouvons émettre l'hypothèse que les personnes ayant un côté innovateur possèdent déjà des bracelets connectés ou ont eu l'occasion d'en essayer. De ce fait, le bracelet leur semble simple d'utilisation.

Nos résultats concernant les deux technologies ont montré des similitudes avec le modèle originel du TAM (Davis, 1989) et le TAM étendue appliqué à l'adoption des NFC (Dutot, 2015). Il est intéressant de noter que contrairement au modèle initial, la seule variable affectant l'intention d'utilisation est l'utilité perçue et ce pour les deux technologies. Cela peut potentiellement s'expliquer par le fait que les technologies touchent au domaine de la santé, domaine où la recherche d'efficience est primordiale comparativement à la simplicité des solutions.

3. Limites de l'étude

Cette étude sur les facteurs d'adoption des objets connectés a ses limites. Premièrement, nous nous sommes uniquement intéressés à la population française qui n'est pas représentative de la population mondiale. Chaque pays possède ses propres environnements culturels et technologiques. Pour étendre et valider cette recherche, cette dernière devrait être réalisée dans d'autres pays. Aussi, notre échantillon représente une population relativement jeune et étudiante, ce qui ne reflète pas la population française de façon globale.

Nous nous sommes intéressés aux facteurs d'adoption de deux objets connectés futuristes liés au domaine de la santé dans le but de mettre en lumière leurs facteurs d'adoption. D'autres variables auraient pu être ajoutées au modèle (design, disponibilité de la technologie, etc.) et il paraît pertinent de penser que les facteurs obtenus puissent différer d'une technologie à une autre. Il conviendra d'adapter ce modèle pour de futures recherches.

IV. Conclusion

Les organisations adaptent leurs stratégies pour faire face aux enjeux et opportunités que représente le big data et la prolifération des données liées à son concept. Nous avons vu que la donnée consommateur est centrale pour les organisations. Le web a d'abord été leur premier gisement avant que les objets connectés fassent leur apparition sur le marché et entraîne avec eux une réelle déferlante de la donnée.

Les entreprises tirent profit de ces informations en se créant des avantages concurrentiels durables et affinent leurs techniques au fil des années grâce à des outils de plus en plus développés. Que cela soit pour l'environnement web ou celui des objets connectés, les moyens de collecte de données sont techniques et bien souvent trop complexes pour le consommateur lambda qui est bien souvent tracé à son insu. Les législations actuelles ne peuvent muter aussi vite que les technologies et c'est donc bien souvent aux entreprises de faire la part des choses en adoptant un comportement qui leur semblent adapté en fonction des lois en vigueur. L'Europe a sa propre législation en termes de données personnelles, mais c'est au niveau international que les décisions devraient être prises aujourd'hui pour garantir un avenir aux futures technologies de demain.

Si l'adoption du web semble être actée, celle des objets connectés n'en reste pas moins un défi pour les années à venir.

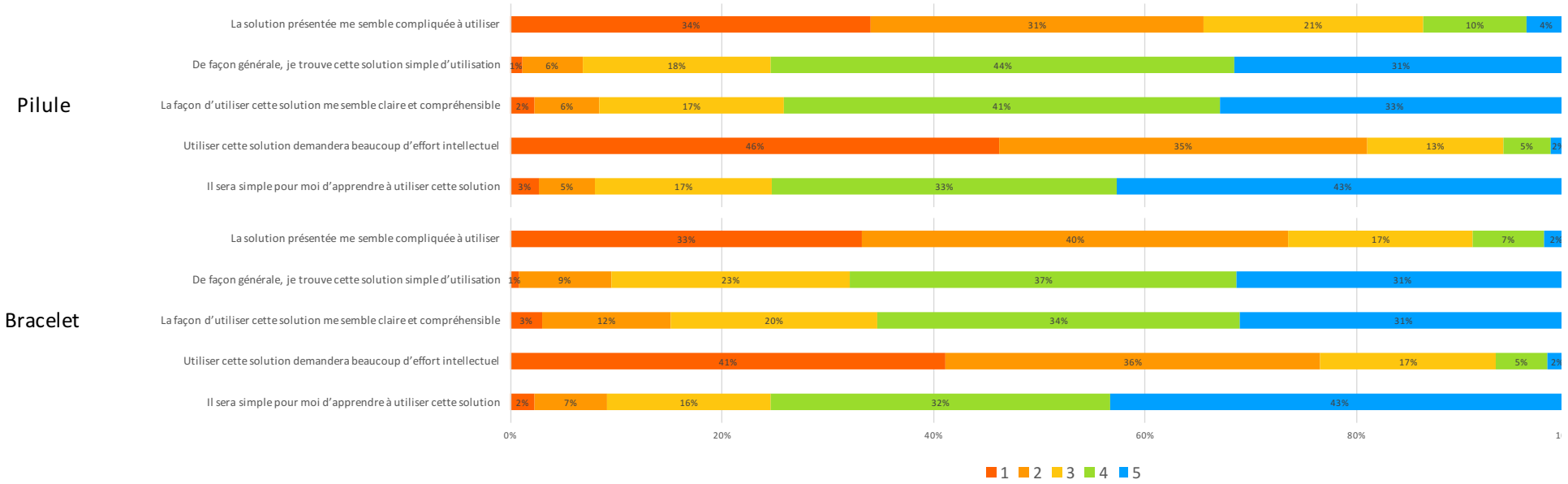
Les consommateurs sont inquiets du nombre et de la nature des données qui sont collectées par les entreprises à leurs sujets. Malgré cela, ils ne sont pas réellement au fait des données qu'ils communiquent avec les organisations, et la majorité d'entre elles décident de garder les individus dans l'incertitude. Cette dynamique a pour seule finalité d'éroder la confiance que les consommateurs ont dans les organisations, et de la nature des données qu'ils souhaitent partager avec elle.

Nous avons pu démontrer dans l'analyse de l'adoption des futurs objets connectés que la confiance est la variable externe la plus importante et essentielle à cette adoption. Pour faciliter cette adoption, les organisations devront également miser sur l'influence sociale de

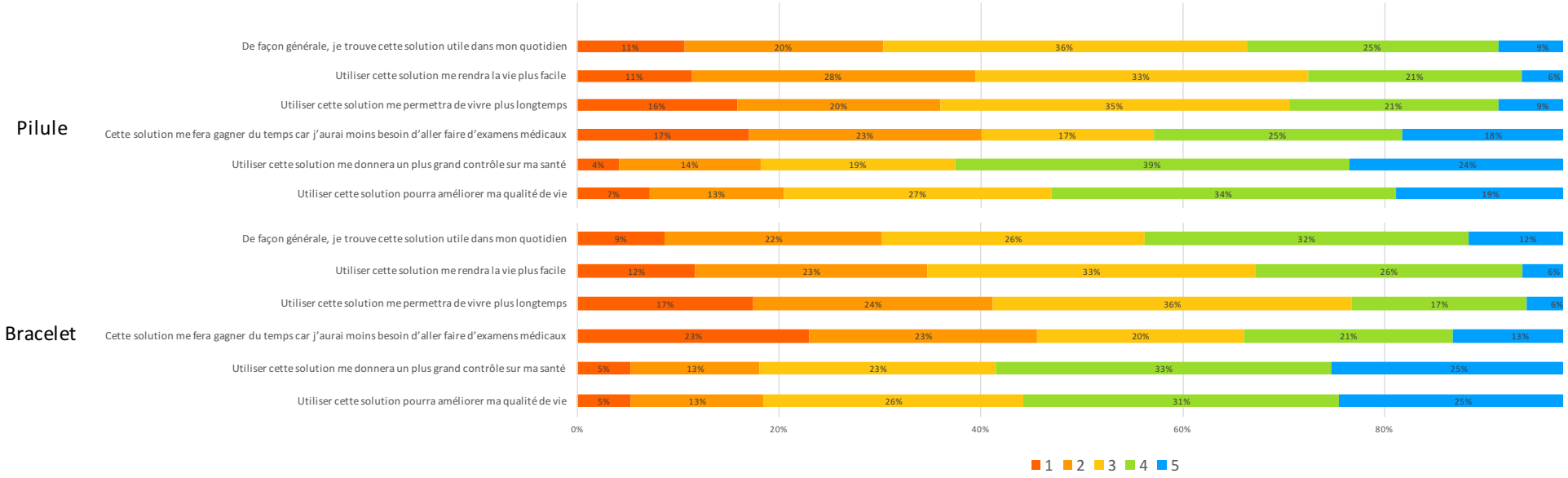
personnalités, sur l'aspect sécuritaire de leurs technologies et des données collectées. Nous avons pu voir que cela soit dans l'environnement web ou celui des objets connectés, la donnée a de la valeur pour l'entreprise, comme pour le consommateur, et tous deux attendent un bénéfice en retour de ces informations. Le consommateur attend une amélioration des produits et des services proposés par les entreprises tout en exigeant que ses données soient confidentielles et que ces dernières ne soient pas facilement accessibles pour des tiers. L'entreprise elle, est à la recherche de données de ses consommateurs à travers différents contextes et plateformes, dans le but de toujours plus personnaliser son offre et de la proposer à la bonne personne, au bon endroit, au bon moment.

La réglementation actuellement en vigueur changera probablement dans les années à venir car entreprises et consommateurs évoluent dans un environnement de plus en plus complexe et propice aux dérives. Outre les réglementations de niveau législatif, c'est aussi le rôle des Universités de sensibiliser à ces dérives. Elles se doivent de proposer des cours d'éthique dans les formations qui ont trait au monde du digital, car ce sont bien elles qui forment les décideurs de demain.

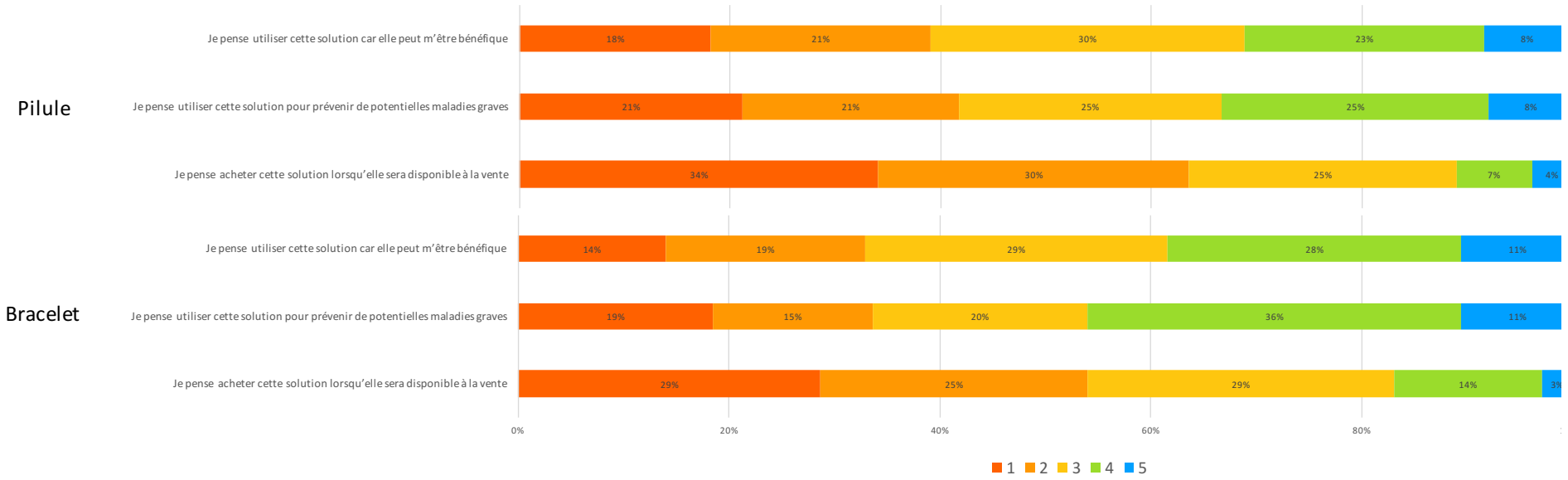
V. Annexes



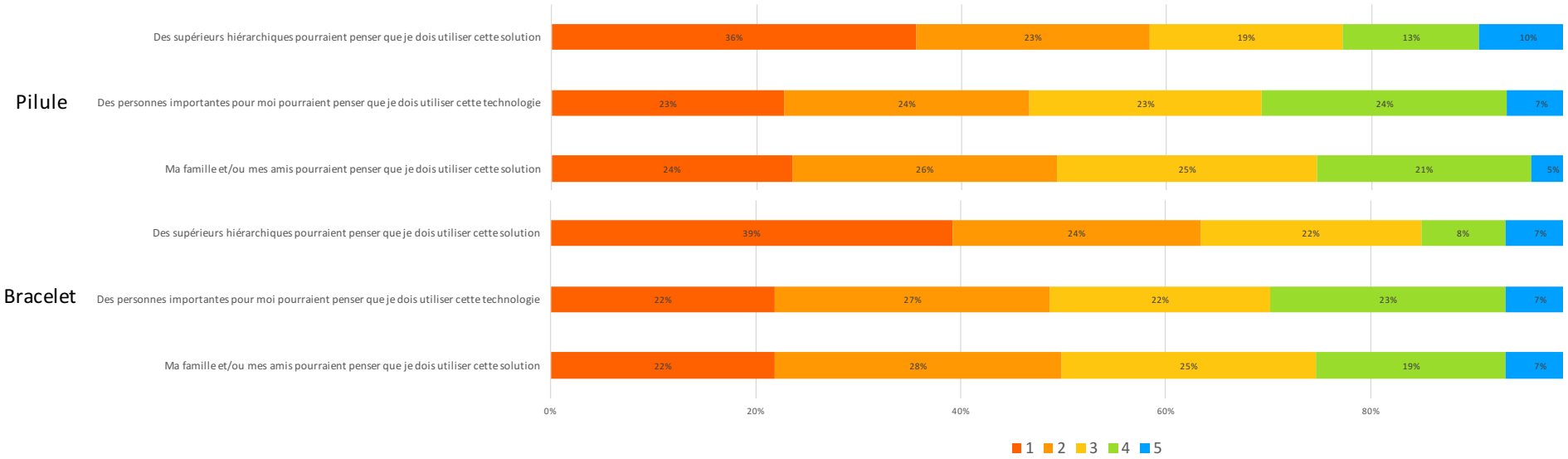
Annexe 1 : Statistiques univariées pour la pilule et le bracelet, simplicité d'utilisation perçue



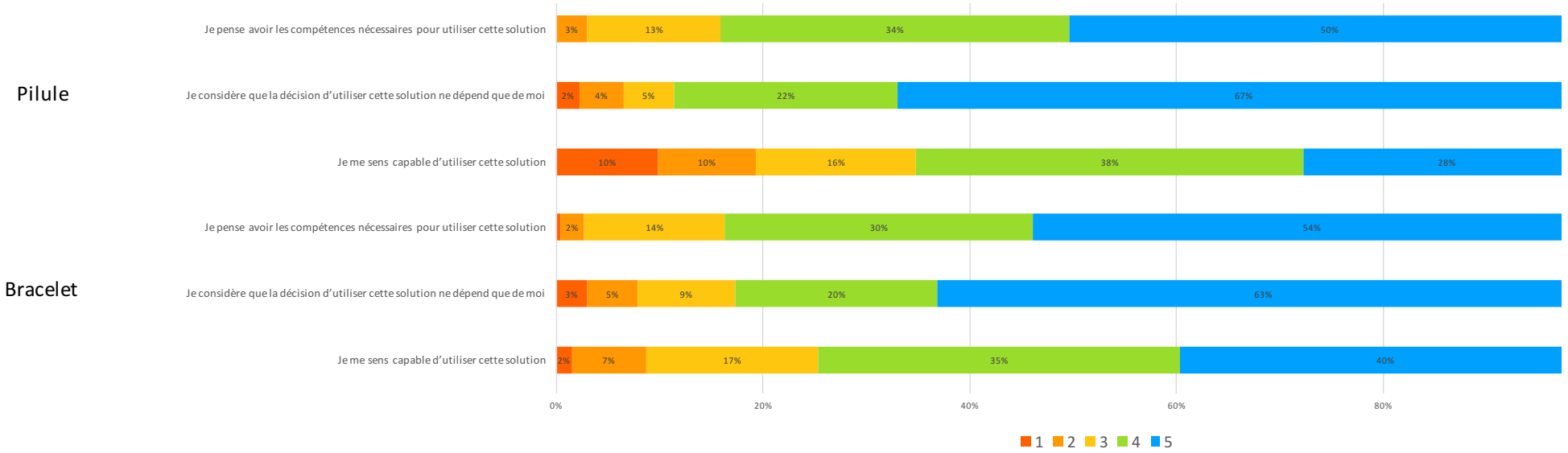
Annexe 2 : Statistiques univariées pour la pilule et le bracelet, utilité perçue



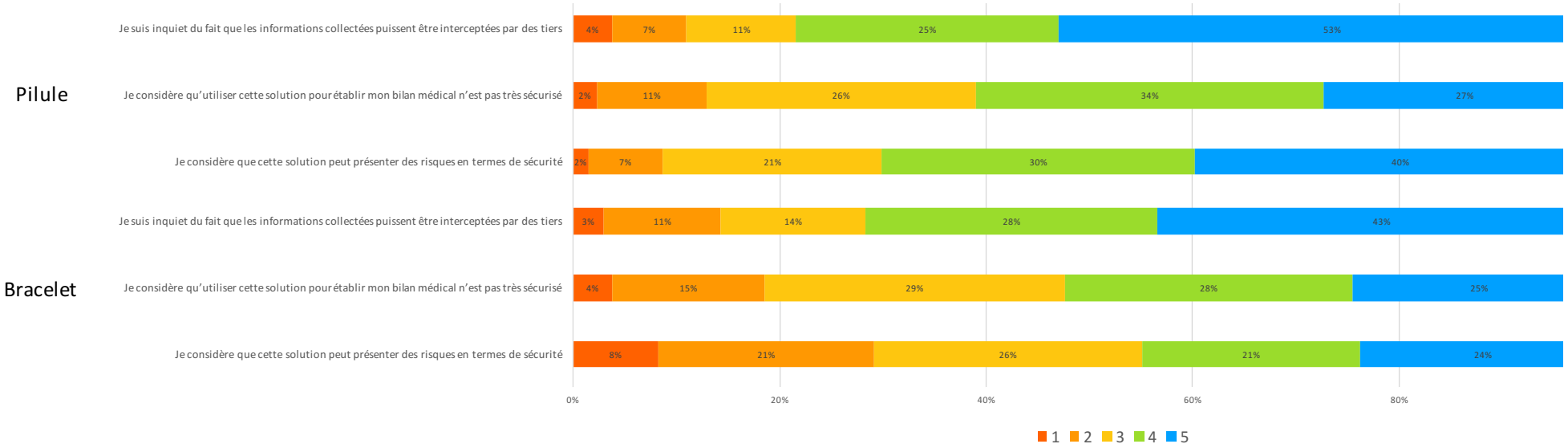
Annexe 3 : Statistiques univariées pour la pilule et le bracelet, intention d'utilisation



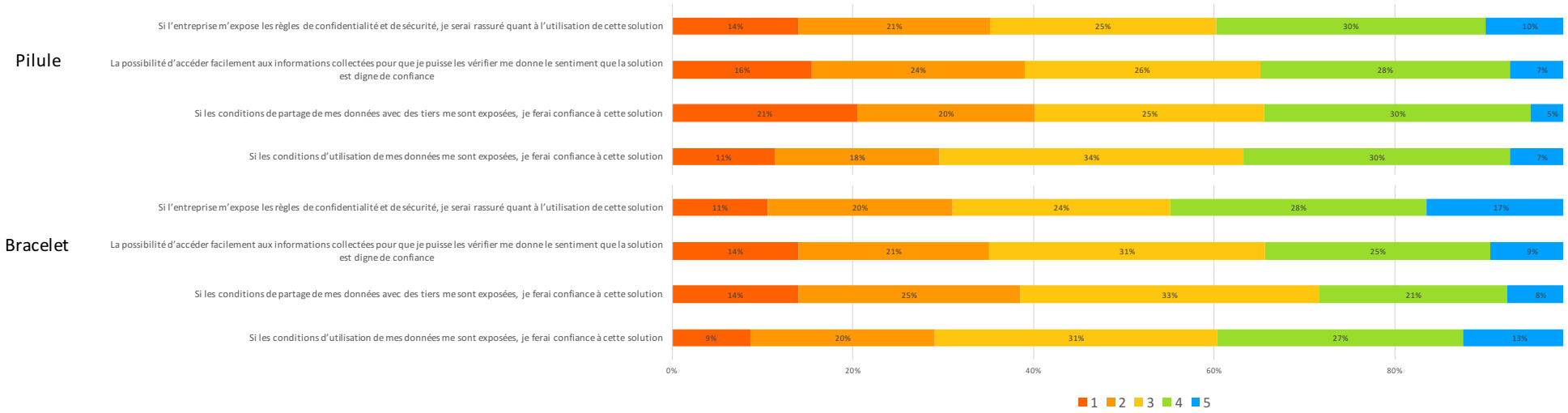
Annexe 4 : Statistiques univariées pour la pilule et le bracelet, influence sociale



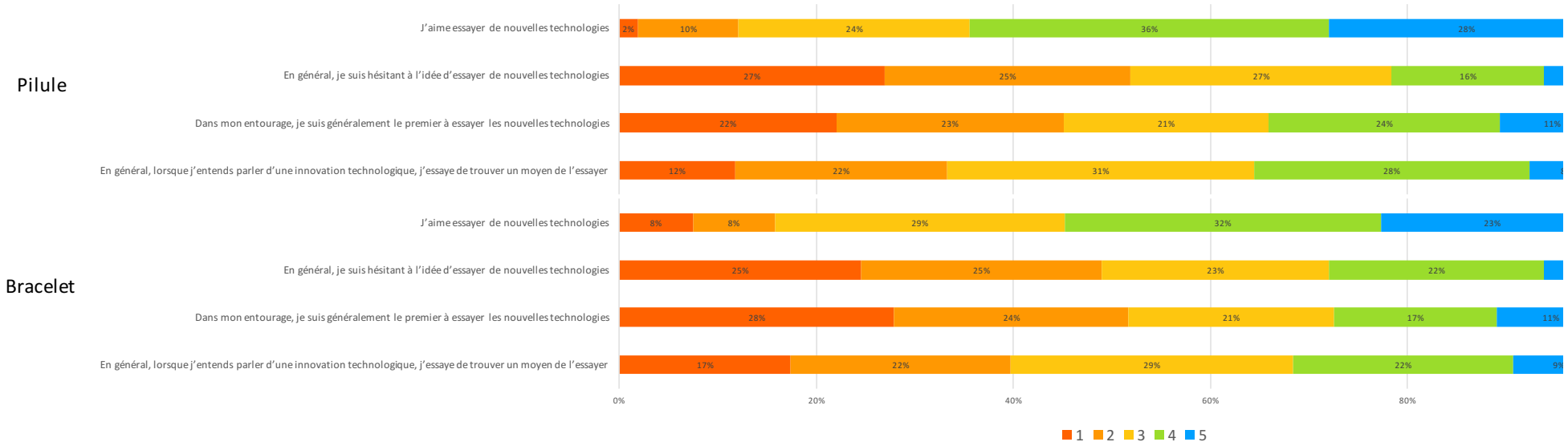
Annexe 5 : Statistiques univariées pour la pilule et le bracelet, utilisation



Annexe 6 : Statistiques univariées pour la pilule et le bracelet, sécurité



Annexe 7 : Statistiques univariées pour la pilule et le bracelet, confiance



Annexe 8 : Statistiques univariées pour la pilule et le bracelet, côté innovateur de l'individu

VI. Bibliographie

Abowd GD, Mynatt ED. Charting past, present, and future research in ubiquitous computing. ACM Trans Comput Hum Interact 2000;7(1):29–58.

Agarwal, R. and Prasad, J. (1998) 'A conceptual and operational definition of personal innovativeness in the domain of information technology', Information Systems Research, 9(2), pp. 204–215. doi: 10.1287/isre.9.2.204.

Ambrosini, V., & Bowman, C. (2009). What are dynamic capabilities and are they a useful construct in strategic management? International Journal of Management Reviews, 11(1), 29–49.

Anderson, C. (2008). The end of theory: The data deluge makes the scientific methodobsolete. Wired (Consulté en le 21 Février 2016, http://archive.wired.com/science/discoveries/magazine/16-07/pb_theory).

Angwin, J. 2010. The web's new gold mine: Your secrets—a journal investigation finds that one of the fastest-growing businesses on the Internet is the business of spying on consumers; first in a series. Wall Street Journal (Eastern Edition)

Angwin, J., and T. McGinty. 2010. What they know: Watching the Web watchers—journal examines top sites in the U.S. to measure 'cookies,' 'beacons' and other trackers. Wall Street Journal (Europe)

Atzori L, Iera A, Morabito G. The internet of things: a survey. Comput Netw 2010;(54):2787–805.

Banker, S. (2014). Amazon and anticipatory shipping: A dubious patent? Forbes (24 Janvier 2014 sur http://www.forbes.com/sites/stevebanker/2014/01/24/amazon-and-anticipatory-shipping-a-dubious-patent/).

Barney, J. B. (2014). How marketing scholars might help address issues in resource-based theory. Journal of the Academy of Marketing Science, 42(1), 24–26

Barney, J. B. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99–120.

Barreto, A.M. (2014). The word-of-mouth phenomenom in the social media era. International Journal of Market Research, 56(5), 631–654.

Bedi, M. 2013. Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply. Boston College Law Review 1

Benn, S.I. 1984. Privacy, Freedom, and Respect for Persons. In Philosophical Dimensions of Privacy: An Anthology. Cambridge, UK: Cambridge University Press.

Beresford AR, Stajano F. Location privacy in pervasive computing. Pervasive Comput IEEE 2003;2(1):46–55.

Borgia, E. (2014) 'The Internet of things vision: Key features, applications and open issues', Computer Communications, 54, pp. 1–31. doi: 10.1016/j.comcom.2014.09.008.

Brink, E. (2015) Car-sharing companies pioneer Internet of things. Disponible sur : http://blogs.ptc.com/2015/03/16/car-sharing-companies-pioneer-internet-of-things/ (Consulté le : 4 Mars 2016).

BVA - Syntec numérique (2014) Baromètre de l'innovation - Un baromètre BVA – Syntec numérique. Disponible sur : http://www.syntec-numerique.fr/sites/default/files/related_docs/barometre_de_linnovation_sn_bva_fevrier2014.pdf (Consulté le : 9 Avril 2016).

Campbell R, Al-Muhtadi J, Naldurg P, Sampemane G, Mickunas MD. Towards security and privacy for pervasive computing. In: Software security – theories and systems. NewYork, Berlin and Heidelberg: Springer; 2003. p. 1–15.

Caprioli, E. (2012) L'adresse IP n'est pas forcément une donnée à caractère personnel. Disponible sur : http://www.lexisnexis.fr/droit-document/article/communication-commerce-electronique/07-2015/064_PS_CCE_CCE1507CM00064.htm#.VtcHhX3hBXE (Consulté le : 2 Mars 2016).

Caron, X., Bosua, R., Mainard, S.B. and Ahmad, A. (2016) 'The Internet of things (IoT) and its impact on individual privacy: An Australian perspective', Computer Law & Security Review, 32(1), pp. 4–15. doi: 10.1016/j.clsr.2015.12.001.

Chen YK. 2012. Challenges and opportunities of internet of things. Asia and South Pacific design automation conference (ASP-DAC), Issue 17, p. 383–8.

Chen, S.C., Chen, H.H., & Chen, M.F. (2009). Determinants of satisfaction and continuance intention towards self-service technologies. Industrial Management + Data Systems, 109(9), 1248–1263.

Chessell, M. (2014) 'Ethics for big data and analytics', IBM, .

CNIL : nos missions (2016) Disponible sur : https://www.cnil.fr/fr/les-missions (Consulté le : 2 Mars 2016).

Cohen, J.E. 2008. Privacy, Visibility, Transparency, and Exposure. University of Chicago Law Review 75(1).

Cookies, tags and Pixels: Tracking customer engagement (2015) Disponible sur : http://www.visualiq.com/resources/marketing-attribution-newsletter-articles/cookies-tags-and-pixels-tracking-customer-engagement (Consulté le : 27 Février 2016).

Culnan MJ, Armstrong PK. Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. Organ Sci 1999;10(1):104–15.

Davenport, T.H. (2014) Big data at work: Dispelling the myths, uncovering the opportunities. Boston: Harvard Business Press.

Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.

Day, G. S. (2014). An outside-in approach to resource-based theories. Journal of the Academy of Marketing Science, 42(1), 27–28.

Day, G. S. (2011). Closing the marketing capabilities gap. The Journal of Marketing, 75(4), 183–195.

Définition du big data - Opportunités du big data - France (2016) Disponible sur : https://www-01.ibm.com/software/fr/data/bigdata/ (Consulté le : 27 Février 2016).

De Montjoye, Y.-A., Hidalgo, C.A., Verleysen, M. and Blondel, V.D. (2013) 'Unique in the crowd: The privacy bounds of human mobility', Scientific Reports, 3. doi: 10.1038/srep01376.

Disney: Making magic through digital innovation (2014) Disponible sur : https://www.fr.capgemini-consulting.com/resource-file-access/resource/pdf/disney_0_0.pdf (Consulté le : 12 Mars 2016).

Doney, P.M., & Cannon, J.P. (1997). An examination of the nature of trust in buyer–seller relationships. Journal of Marketing, 61(2), 31–35.

Ducourtieux, C. (2015) « safe harbor »: Que change l'arrêt de la justice européenne sur les données personnelles ?. Disponible sur : http://www.lemonde.fr/pixels/article/2015/10/06/safe-harbor-que-change-l-arret-de-la-justice-europeenne-sur-les-donnees-personnelles_4783686_4408996.html (Consulté le : 19 Mars 2016).

Duhigg, C. (2012). How companies learn your secrets. New York Times (Publié le 16 Février 2012 sur http://www.nytimes.com/2012/02/19/magazine/shoppinghabits.html) (Consulté le : 23 Mars 2016)

Dutot, V. (2014). Adoption of social media using technology acceptance model: The generational effect. International Journal of Technology and Human Interaction, 10(4), 18–35

Dutot, V., Factors influencing Near Field Communication (NFC) adoption: An extended TAM approach, Journal of High Technology Management Research (2015), http://dx.doi.org/10.1016/j.hitech.2015.04.005 (Consulté le : 22 Janvier 2016)

Droit au déréférencement: Rejet du recours gracieux formé par Google à l'encontre de la mise en demeure (2015) Disponible sur : https://www.cnil.fr/fr/droit-au-dereferencement-

rejet-du-recours-gracieux-forme-par-google-lencontre-de-la-mise-en-demeur-0 (Consulté le : 3 Mars 2016).

Eckersley, P. (2010) 'How unique is your web browser?', Proceedings of the Privacy Enhancing Technologies Symposium, pp.1–18..

Erevelles, S., Horton, V., & Fukawa, N. (2007). Imagination in marketing. Marketing Management Journal, 17(2), 109–119

Erevelles, S., Fukawa, N. and Swayne, L. (2016) 'Big data consumer analytics and the transformation of marketing', Journal of Business Research, 69(2), pp. 897–904. doi: 10.1016/j.jbusres.2015.07.001.

Eriksson, K., Kerem, K., & Nilsson, D. (2005). Customer acceptance of internet banking in Estonia. International Journal of Bank Marketing, 23(2), 200–216.

Etzioni, A. 2012. The Privacy Merchants: What is to Be Done? University of Pennsylvania Journal of Constitutional Law 14(4): 929.

Eudes, Y. (2016) Transfert de données personnelles: Un « accord bouclier » entre États-Unis et Europe critiqué. Disponible sur : http://www.lemonde.fr/pixels/article/2016/02/03/transfert-de-donnees-personnelles-un-accord-bouclier-entre-etats-unis-et-europe-critique_4858647_4408996.html (Consulté le : 19 Mars 2016).

Faith Cranor, L., Hoke, C., Giovanni Leon, P. and Au, A. (2014) Are They Worth Reading? An In-Depth Analysis of Online Advertising Companies' Privacy Policies. .

Festinger, L. (1962). A theory of cognitive dissonance (2nd ed.). Stanford University Press.

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention and behaviour: An introduction to theory and research. Reading, MA: Addison-Wesley.

Flavian, C., Guinaliu, M., & Torres, E. (2006). How bricks-and-mortar attributes affect online banking adoption. International Journal of Bank Marketing, 24(6), 406–423.

Flynn, L. R. and R. E. Goldsmith, “A Validation of the Goldsmith and Hofacker Innovativeness Scale,” Educational and Psychological Measurement, 53, (1993), 1105–1116

García, Ó.M., Martín, J.M. and Aubert, D.G. (2012) ‘Detecting browser fingerprint evolution for identifying unique users’, International Journal of Electronic Business, 10(2), p. 120. doi: 10.1504/ijeb.2012.051116.

Gartner (2016) Gartner says personal worlds and the Internet of everything are Colliding to create new markets. Disponible sur : http://www.gartner.com/newsroom/id/2621015 (Consulté le : 9 Avril 2016).

Gefen, D., Karahanna, E., & Straub, D.W. (2003). Trust and TAM in online shopping: an integrated model. MIS Quarterly, 27(1), 51–90.

Georges, B. (2014) Google parie sur les nanotechnologies. Disponible sur : http://www.lesechos.fr/29/10/2014/LesEchos/21803-081-ECH_sante---google-parie-sur-les-nanotechnologies.htm (Consulté le : 12 Mars 2016).

Google fait un pas vers le ‘droit à l’oubli’ réclamé par l’UE (2016) Disponible sur : http://www.capital.fr/a-la-une/actualites/google-fait-un-pas-vers-le-droit-a-l-oubli-reclame-par-l-ue-1102557 (Consulté le : 3 Mars 2016).

Havas Media (2014), Les Français et leurs datas. Disponible sur : http://www.havasmediaopendata.com/#projectWrapper (Consulté le : 10 Avril 2016)

HP news - HP study reveals 70 percent of Internet of things devices vulnerable to attack (2014) Disponible sur : http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.Vu7COOLhDIV (Consulté le : 20 Mars 2016).

Impact de la vie privée sur les résultats de recherche (2016) Disponible sur : https://www.google.com/transparencyreport/removals/europeprivacy/ (Consulté le : 3 Mars 2016).

Intel (2016) Intel security’s international Internet of things smart home survey shows many respondents sharing personal data for money | Intel newsroom. Disponible sur :

https://newsroom.intel.com/news-releases/intel-securitys-international-internet-of-things-smart-home-survey/ (Consulté le : 10 Avril 2016).

Jeyaraj, A., Rottman, J., & Lacity,M. (2006). A review of the predictors, linkages, and biases in IT innovation adoption research. Journal of Information Technology, 21(1), 1–23.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. Business Horizons, 53(1), 59—68.

Kelly, H. 2013. On Data Privacy Day, Twitter and Google focus on Government Requests. CNN, Janvier 28. http://www.cnn.com/2013/01/28/tech/social-media/dataprivacy-day/ (Consulté le : 2 Avril 2016)

King, R. (2012). Ford gets smarter about marketing and design. Wall Street Journal (Publié le 1er Février 2016 sur http://blogs.wsj.com/cio/2012/06/20/ford-getssmarter-about-marketing-and-design/).

Kirton, M., Adaptors and Innovators: A Description and Measure, J. Applied Psychology, 61, 5 (1976), 622–629.

Lancelot-Miltgen, C. and Lemoine, J.-F. (2015) 'Mieux collecter les données personnelles sur Internet. Une étude qualitative auprès d'internautes français', Décisions Marketing, 79, pp. 35–52. doi: 10.7193/dm.079.35.52.

La Poste Solutions Business (2014) Objets connectés : ce qu'en attendent les français. Disponible sur : http://www.docapost.com/wp-content/uploads/2015/01/infographie-la-poste-generique.pdf (Consulté le : 9 Avril 2016).

Le droit au déréférencement (no date) Disponible sur : https://www.cnil.fr/fr/le-droit-au-dereferencement (Consulté le : 3 Mars 2016).

Les moteurs de recherche (2016) Disponible sur : https://www.cnil.fr/fr/les-moteurs-de-recherche (Consulté le : 3 Mars 2016).

Lee, I. and Lee, K. (2015) 'The Internet of things (IoT): Applications, investments, and challenges for enterprises', Business Horizons, 58(4), pp. 431–440. doi: 10.1016/j.bushor.2015.03.008.

Liu, C., Marsewka, J.T., Lu, J., & Yu, C. -S. (2004). Beyond concern: A privacy–trust–behavioral intention model of electronic commerce. Information & Management, 42,127–142.

Loftus, T. 2011a. Experts Investigate Carrier IQ Fears. Wall Street Journal http://blogs.wsj.com/digits/2011/12/02/experts-investigate-carrier-iq-fears/ (Consulté le : 10 Mars 2016)

Ma, X., Yao, X., & Xi, Y. (2009). How do interorganizational and interpersonal networks affect a firm's strategic adaptive capability in a transition economy? Journal of Business Research, 62(11), 1087–1095.

Mason RO. Four ethical issues of the information age. MISQ 1986;5–12.

Mauritius declaration on the Internet of Things (2014) Disponible sur : http://www.privacyconference2014.org/media/16596/Mauritius-Declaration.pdf (Consulté le : 26 Mars 2016).

McNeely, C.L. and Hahm, J. (2014) 'The big (data) bang: Policy, prospects, and challenges', Review of Policy Research, 31(4), pp. 304–310. doi: 10.1111/ropr.12082.

Md Nor, K., Barbuta-Misu, N., & Stroe, R. (2011). A model for analysing the determinant factors of adoption e-banking services by Romanian customers. Academic Computation & Economic Cybernetics Studies & Research, 45(4), 1–18

Mitchell, I.D. (2012) 'Third-Party tracking cookies and data privacy', SSRN Electronic Journal, doi: 10.2139/ssrn.2058326.

Morey, T., Forbath, T. 'Theo' and Schoop, A. (2015) Customer data: Designing for transparency and trust. Disponible sur : https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust (Consulté le : 12 Mars 2016).

Nasri, W., & Charfeddine, L. (2012). Factors affecting the adoption of Internet banking in Tunisia: An integration theory of acceptance model and theory of planned behavior. The Journal of High Technology Management Research, 23(1), 1–14.

Nissenbaum, H. 2009. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford, CA: Stanford University Press

Nissenbaum, H. (2011) 'A Contextual approach to privacy online', Daedalus, 140(4), pp. 32–48. doi: 10.1162/daed_a_00113.

Nunan, D. and Di Domenico, M. (2013) 'Market research and the ethics of big data', International Journal of Market Research, 55(4), p. 505. doi: 10.2501/ijmr-2013-015.4

Oriwoh E, Sant P, Epiphaniou G. Guidelines for internet of things deployment approaches–the thing commandments. Procedia Comput Sci 2013;(21):122–31

Pictures of the Future, The Magazine for Research and Innovation (2012) Disponible sur : http://www.siemens.com/content/dam/internet/siemens-com/innovation/pictures-of-the-future/pof-archive/pof-fall-2012.pdf (Consulté le : 9 Avril 2016).

Radomir, L., & Nistor, V.C. (2013). An application of technology acceptance model to internet banking services. Proceedings of the 6th international conference "marketing — from information to decision" (pp. 251–266).

Reynaud, F. (2016) Le conflit entre apple et le FBI arrive au Parlement français. Disponible sur : http://www.lemonde.fr/pixels/article/2016/03/03/le-debat-entre-apple-et-le-fbi-s-exporte-au-parlement-francais_4876147_4408996.html (Consulté le : 8 Mars 2016).

Ring, T. (2015) 'Keeping tabs on tracking technology', Network Security, 2015(6), pp. 5–8. doi: 10.1016/s1353-4858(15)30047-7.

Rupanjali, N., Bhal, K.T., & Kapoor, G.T. (2013). Factors influencing IT adoption by bank employees: An extended TAMapproach. Vikalpa: The Journal of Decision Makers, 38(4), 83–96.

Sadilek, A., & Krumm, J. (2012). Proceedings from AAAI Conference on Artificial Intelligence 2012: Far Out: Predicting Long-Term Human Mobility. North America.

Santé: Google parie sur les nanotechnologies (2014) Disponible sur : http://www.lesechos.fr/29/10/2014/LesEchos/21803-081-ECH_sante---google-parie-sur-les-nanotechnologies.htm#1IlWBOX3y65HKl5o.99 (Consulté le : 27 Février 2016).

Satell, G. (2014). 5 thingsmanagers should knowabout the big data economy. Forbes publié le 26 janvier 2014. sur http://www.forbes.com/sites/gregsatell/2014/01/26/5-things-managers-should-know-about-the-big-data-economy/). (Consulté le 1 Février 2016)

Smith HJ, Dinev T, Xu H. Information privacy research: an interdisciplinary review. MISQ 2011;35(4):989–1016.

Soper, D.S. (2014). A-priori sample size calculator for structural equation models [software]. Disponible sur http://www.danielsoper.com/statcal (Consulté le : 22 Février 2016)

Steinbach, P. (2012). Dynamic pricing pinpoints market value. Athletic Business (Disponible sur : www.athleticbusiness.com/articles/article.aspx?articleid=3909&zoneid=34).

Swan, M. (2013) 'The quantified self: Fundamental disruption in big data science and biological discovery', Big Data, 1(2), pp. 85–99. doi: 10.1089/big.2012.0002.

Tan, G.W. -H., Sim, J. -J., Ooi, K. -B., & Phusavat, K. (2012, Spring). Determinants of mobile learning adoption: An empirical analysis. Journal of Computer Information Systems, 82–91.

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. Strategic Management Journal, 28(13), 1319–1350

Tene, O., and J. Polonetsky. 2012. Privacy in the Age of Big Data: A Time for Big Decisions. Stanford Law Review 64:63.

Texas Instrument (no date) Application areas for the Internet of things. Disponible sur : http://www.ti.com/ww/en/internet_of_things/iot-applications.html (Consulté le : 21 Février 2016).

TRUSTe Internet of things privacy index - US edition (2015) Disponible sur : https://www.truste.com/resources/privacy-research/us-internet-of-things-index-2014/ (Consulté le : 20 Mars 2016).

Uber to share ridership data with Boston - the Boston globe (2015) Disponible sur : https://www.bostonglobe.com/business/2015/01/13/uber-share-ridership-data-with-boston/4Klo40KZREtQ7jkoaZjoNN/story.html (Consulté le : 3 Mars 2016).

Van der Meulen, R. (2016) Gartner Says 6.4 Billion Connected 'Things' Will Be in Use in 2016, Up 30 Percent From 2015. Disponible sur : http://www.gartner.com/newsroom/id/3165317 (Consulté le : 3 Mars 2016).

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. Decision Sciences, 39(2), 273–315.

Venkatesh, V., & Davis, F.D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management Science, 46(2), 186–204.

Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425–478.

Vermesan O, Friess P, Guillemin P, Gusmeroli S, Sundmaeker H, Bassi A, et al. Internet of things strategic research roadmap. Internet Things Glob Technol Soc Trends 2011;9–52.

Viaene, S. (2013). Data scientists aren't domain experts. IT Professional, 15(6), 12–17

Wang, Y., Wang, Y., Lin, H., & Tang, T. (2003). Determinants of user acceptance of Internet banking: An empirical study. International Journal of Service Industry Management, 14(5), 501–519.

Weber RH. Internet of things–new security and privacy challenges. Comput Law Secur Rev 2010;1(26):23–30.

Weber, R.H. (2015) 'Internet of things: Privacy issues revisited', Computer Law & Security Review, 31(5), pp. 618–627. doi: 10.1016/j.clsr.2015.07.002.

Weinberg, B.D., Milne, G.R., Andonova, Y.G. and Hajjat, F.M. (2015) 'Internet of things: Convenience vs. Privacy and secrecy', Business Horizons, 58(6), pp. 615–624. doi: 10.1016/j.bushor.2015.06.005.

What are Internet cookies and what do cookies do? (2008) Disponible sur : http://www.webopedia.com/DidYouKnow/Internet/all_about_cookies.asp (Consulté le : 27 Février 2016)

World Internet users statistics and 2015 world population stats (2015) Disponible sur : http://www.internetworldstats.com/stats.htm (Consulté le : 12 Mars 2016).

Yousafzai, S.Y., Pallister, J.G., & Foxall, G.R. (2003). A proposed model of E-trust for electronic banking. Technovation, 23, 847–860.