UCLouvain

LOUVAIN
School of Management

Louvain School of Management

L’impact du RGPD sur la confiance des consommateurs

Auteur : Donatien Mercier
Promoteur(s) : Chantal de Moerloose
Année académique 2018-2019

Je tiens à remercier chaleureusement toutes les personnes qui, de près ou de loin, ont permis la concrétisation de cinq années d'étude représentées par le présent mémoire.

Plus particulièrement, je souhaite adresser mes remerciements les plus sincères envers ma promotrice, Chantal de Moerloose, dont l'écoute, l'expertise et les précieux conseils sont traduits dans les pages à suivre.

Par ailleurs, je suis reconnaissant de l'enseignement de qualité reçu de l'ensemble du corps académique tout au long de ce périple universitaire.

Je remercie également les personnes ayant pris la peine de consacrer leur temps en répondant au questionnaire indispensable à l'analyse de notre étude.

En outre, mon souhait est de mettre en lumière le travail de l'ombre exercé par l'équipe ayant mis sur pied le séminaire d'accompagnement du mémoire (LLSMD2094) en tant qu'outil pédagogique.

Enfin, une pensée particulière envers mes proches, amis et famille dont le soutien sans faille fut hautement apprécié lors de cette épreuve exigeante en ressources psychologiques.

Table des matières

Introduction **1**
Environnement- Contexte 1
Question de recherche 3
Sous-questions 3
Motivation managériale 4
Motivation scientifique 5
Motivation sociétale et éthique 5

Partie 1 : Le contenu du RGPD **6**
Chapitre 1 : Le droit à la portabilité des données **6**
Énoncé du droit 6
Réduction des switching costs 7
IIa. Réduction de l'effet de "lock-in" 9
Effet réseau 10
Points d'attention pour les consommateurs comme entreprises 11
Chapitre 2 : Le droit à la rectification des données **11**
Énoncé du droit 11
Types de données erronées 12
Amélioration de la qualité des données 13
Customer relationship management 15
Points d'attention pour les entreprises 16
Chapitre 3 : Le droit à l'effacement des données **17**
Contexte n°1 17
Énoncé du droit 17
Génération Z et vie privée en ligne 18
Contexte n°2 20
Personal Branding 20
Traitement illicite de données 22
Chapitre 4 : Le droit d'accès à l'information **23**
Énoncé du droit 23
Marketing de label 24
Le commerce des data-brokers 26
Data protection officer 27
Points d'attention pour les citoyens européens 29

Chapitre 5 : Le droit d'opposition au traitement **30**
Énoncé du droit 30
Profilage et display advertising 30
Marketing automation 32
Personnalisation des e-mails et click through rate 34
Points d'attention pour les entreprises 35
Chapitre 6 : Le droit de limitation au traitement **36**
Énoncé du droit 36
Le cyberbullying 36
Chapitre 7 : Hypothèses à tester **38**

Partie 2 : Étude quantitative **40**
Chapitre 1 : La méthodologie **40**
Collecte des données 40
Questionnaire 40
Échelles de mesure 41
Échantillon 42
Tableau de croisement Hypothèses - Questions 43
Chapitre 2 : Analyse des résultats **44**
Préparation des données 44
Analyse descriptive de l'échantillon 44
Analyse de la fiabilité des échelles 47
Échelle de compréhension 48
Échelle d'appréciation 48
Analyse en composantes principales 49
Compréhension du RGPD 50
Appréciation du RGPD 52
Vérification des hypothèses de l'étude 53
Hypothèses principales 53
Connaissance des outils juridiques par caractéristiques des répondants 59
Compréhension des outils juridiques par caractéristiques des répondants 60
Appréciation des outils juridiques par caractéristiques des répondants 62
Récapitulatif des résultats 65

Partie 3 : Conclusions **68**
Conclusion de l'étude 68
Implications managériales, éthiques et scientifiques 70
Limites de l'étude 71
Futures recherches 72

Bibliographie **73**

Annexes **84**

Introduction

I. Environnement- Contexte

À l'heure actuelle, les progrès technologiques qui façonnent notre ère posent la question de nombreux défis, notamment en matière de protection des données à caractère personnel. Le caractère personnel d'une donnée se définit comme étant « toute information se rapportant à une personne physique identifiée ou identifiable » à l'image d'un nom, de données de localisation, d'un identifiant en ligne ou encore de données propres à l'identité physique, comportementale ou psychologique (Article 4, RGPD).

Ainsi, l'essor des activités en ligne telles que les forums de discussion, les réseaux sociaux, l'échange de courriels ou encore la simple consultation de pages web, simplifie le partage d'informations à caractère personnel et rend possible toutes formes de diffusion publique de ce contenu, à l'échelle mondiale (SPF économie, 2018). Dans cet ordre d'idées, les « systèmes destinés à stocker, traiter et diffuser des données pour les particuliers comme pour les administrations» (Mosco, 2014), à l'instar du *cloud computing*, amènent à amoindrir le contrôle qu'un particulier détient sur ses propres informations sensibles (SPF économie, 2018). À titre d'illustration, en janvier 2018, le Belge moyen passe environ 5 heures par jour à utiliser des devises et services connectés à internet, ce qui augmente considérablement la fenêtre temporelle d'échange de données (cf. Annexe n°1).

En parallèle, les formes de collecte d'informations personnelles tendent à se sophistiquer, celles-ci se sont complexifiées de telle sorte à les rendre moins détectables. Ainsi, il est commun que des informations nécessaires à l'établissement d'un profil type d'internaute remontent jusqu'aux serveurs sans même que le visiteur n'ait eu l'occasion d'en être informé. La technique de collecte la plus communément utilisée est le recours aux cookies, qui enregistrent étape après étape, le cheminement sur la toile. Cependant, bien que derrière ces procédés de collecte avancés, se cachent les intérêts des entreprises en matière

d'adaptation sur mesure de l'offre, il est aussi probable que ces données soient traitées à des fins de discrimination ou de remaniement de l'information émise (SPF économie 2018).

En outre, il convient de s'intéresser tout particulièrement aux implications pratiques qu'un domaine d'intérêt tel que le Big data, entendu au sens de « données numériques de masse », engendre dans la vie quotidienne des citoyens aux quatre coins du monde (Boyadjian & al., 2018). Dès lors, comment ne pas aborder l'affaire « Cambridge Analytica - Facebook ».

C'est ainsi que fin mars 2018, débute un scandale dont l'ampleur deviendra rapidement internationale et ébranlera l'image du mastodonte Facebook. Tout commence par les révélations troublantes émises par un lanceur d'alerte canadien, du nom de Christopher Wylie, ancien directeur de recherche à Cambridge Analytica, firme britannique d'exploitation de données à des fins stratégiques. En transmettant des documents probants au journal l'Observer de Londres, le Canadien tente de démontrer que les données de millions d'utilisateurs de Facebook ont été utilisées afin d'influencer l'adhésion aux idées électorales de Donald Trump lors de sa campagne présidentielle de 2016 (Manokha, 2018).

Par ailleurs, il est assez révélateur de constater que Steve Bannon, ancien conseiller de Donald Trump, a figuré dans le conseil d'administration de Cambridge Analytica (Astié & al., 2017). À l'origine, une faille de sécurité d'une application intégrée au réseau social a permis illégalement le transfert de données vers Cambridge Analytica. Malgré les regrets exprimés par Marc Zuckerberg, CEO de Facebook, quant aux manquements liés à la protection des données de ses utilisateurs, le cours de bourse du géant du NASDAQ aura tout de même chuté de 19% le 26 juillet 2018, soit l'équivalent de 119 milliards de dollars de capitalisation boursière (Korinman, 2017).

Après la mise en lumière sur cette affaire fortement médiatisée, il est possible de construire un lien ténu entre le « Cambridge Analytica gate » et le bouclier législatif du RGPD. De fait, au cœur du scandale se trouve le transfert non consenti de données sensibles au niveau personnel de 87 millions de victimes dont 2,7 millions résidant dans l'Union européenne (Mugnier, 2018).

À l'image de la connotation politique cachée derrière l'exploitation illégale de ces données, Cambridge Analytica avait en sa possession des données recueillies sur Facebook susceptibles de dresser un profil psychologique enclin à être séduit par la campagne républicaine de Trump. C'est ainsi que, stratégiquement et selon le mode électoral indirect des grands électeurs aux États-Unis, une campagne présidentielle ciblée aux territoires susceptibles de basculer en faveur des républicains était suffisante pour ériger Trump au pouvoir (Manokha, 2018).

II. Question de recherche

« L'impact du *Règlement Général sur la Protection des Données (RGPD)* sur la confiance des consommateurs. »

La finalité du présent mémoire est de déterminer l'influence du RGPD sur la confiance des consommateurs, mesurée par la propension de ces derniers à partager leurs données personnelles aux responsables de traitement dont ils sont les utilisateurs au quotidien.

III. Sous-questions

- Parmi les six principes identifiés du RGPD, lesquels créent le plus ou le moins la confiance chez les consommateurs ?

Différents paramètres sont susceptibles de faire varier le niveau de confiance des consommateurs, à l'instar du contexte économique belge, du taux de chômage, de la situation financière de l'individu ou encore de son épargne. (Dujardin, 2019) Néanmoins, concentrons-nous ici sur la mesure de l'impact relatif des principes les uns par rapport aux autres, enclins à faire varier le degré de confiance des consommateurs.

- La confiance des consommateurs envers le RGPD est-elle influencée par des variables sociodémographiques ?

Est-ce que l'âge et/ou le niveau d'étude influencerai(en)t la propension à partager les données personnelles ? Autrement formulé, des individus disposant d'un esprit davantage critique seraient-ils plus enclins à ne pas consentir au partage de données ?

- L'introduction d'une première variable comportementale comme la réticence préalable au partage de données est-elle inhibée par l'existence d'un label certifié "GDPR compliant" ?

En d'autres termes, est-ce que les personnes qui de prime abord sont réticentes à divulguer leurs données personnelles, reviennent sur leur décision à la vue d'un logo de conformité aux principes du RGPD ?

- L'introduction d'une seconde variable comportementale comme l'addiction au smartphone influence-t-elle l'appréciation ou la connaissance des outils juridiques mis en place par le RGPD ?

En d'autres termes, est-ce que le fait d'être plus fréquemment disponible à la collecte de données personnelles, engendre une prise de conscience des consommateurs face aux vices de l'ère numérique, traduite par une volonté supérieure de recourir aux droits des personnes concernées ?

IV. Motivation managériale

Étant donné la formation étoffée en gestion qu'offre le programme de Master de la Louvain school of management, le profil de sortie des étudiants est, à terme, d'occuper un poste à responsabilités dans la direction et la gestion des entreprises. Dès lors, l'entrée en vigueur du RGPD est interpellante puisque nombreux sont les départements exploitant les données : RH, marketing, comptabilité,... Puisqu'au royaume du marketing, le client est roi, il

convient de déterminer si la sécurisation des données de nos consommateurs est capable d'améliorer l'expérience client en redonnant le contrôle qu'ont les individus sur leurs données personnelles. Ce mémoire a également pour but de procurer des recommandations aux managers et marketers, désireux de mieux appréhender et d'optimiser l'application des principes du RGPD afin d'augmenter la confiance que les consommateurs perçoivent envers leurs produits ou services.

V. Motivation scientifique

Souligner l'existence d'un lien de causalité entre le RGPD et la confiance des consommateurs envers des produits ou services récoltant des données apparaîtrait telle une modeste contribution à ce vaste thème juridique encore peu lié au marketing. En effet, jusqu'alors rares sont les recherches explorant notamment l'effet des stratégies de co-branding par le label de conformité au RGPD. Enfin, cette étude propose une grille de lecture pratique de l'impact marketing du RGPD, en mesurant les différentes intensités du lien de causalité entre chaque principe du texte juridique de cadre européen et la confiance des consommateurs.

VI. Motivation sociétale et éthique

Dans une industrie digitale en constante évolution dont la récolte de données est souvent la clé de modèles d'affaires particulièrement rémunérateurs, de nombreuses dérives violant le droit à la vie privée sont possibles. Ainsi, un acronyme représente le pouvoir tout puissant des géants américains du marché digital : celui de GAFAM (Google, Apple, Facebook, Amazon, Microsoft). L'évolution de l'environnement digital est si disruptive qu'un nouvel acronyme est déjà bien ancré dans la conscience collective, celui de NATU (Netflix, Airbnb, Tesla et Uber).

Avec une puissance financière semblable à la totalité du budget de l'état français pour l'exercice 2017, GAFA est, avec ses 375 milliards de dollars de cumul de trésorerie, propice aux abus de pouvoir au même titre que certains états (Bertholet et Létourneau, 2017). C'est ainsi qu'en mai 2018, une association française de défense des internautes, sous le nom de « Quadrature du Net », a rassemblé près de 12 000 plaintes à l'encontre des GAFAM,

utilisant à bel escient le levier de telles actions collectives permises par le RGPD (Jocard, 2018). Au cœur de la polémique, le processus utilisé par Facebook et Google pour recueillir le consentement des utilisateurs. En particulier, ces plaintes souhaitaient adresser le problème des « cases pré-cochées ou encore des clauses stipulant que la continuation de l'utilisation du service vaut acceptation » (Jocard, 2018).

C'est pourquoi, ce travail académique s'attèle à souligner, pour les managers comme pour les consommateurs, de quelle manière le bouclier législatif du RGPD peut prévenir les abus de pouvoir des nouveaux modèles économiques. De manière que, la responsabilité sociétale engagée par l'utilisation de cette législation dans le quotidien des entreprises, autorise les consommateurs à vivre une expérience en toute transparence.

Partie 1 : Le contenu du RGPD

En l'occurrence, le règlement général sur la protection des données contient 6 principes de base, déclinés en sous-principes suite à une revue transversale de la littérature.

Chapitre 1 : Le droit à la portabilité des données

I. Énoncé du droit

Selon l'article 20 du règlement général sur la protection des données, le droit à la portabilité des données confère aux individus européens la capacité de recevoir leurs données personnelles sous un format structuré, communément utilisé et lisible par machine. Les personnes concernées sont ensuite libres de faire voyager leurs données vers d'autres systèmes de traitement, en vue d'une réutilisation à d'autres fins (Article 20, RGPD).

Le développement des plateformes digitales connaît un essor fulgurant. En 2019, les cinq entreprises leaders en capitalisation boursière sont toutes des plateformes : Apple, Google, Microsoft, Amazon et Facebook (Forbes Magazine, 2019).

Si les prévisions actuelles se confirment, la part des plateformes dans le revenu net de l'indice boursier S&P pourrait être de 50% d'ici 2042 (Manokha, 2018).

La portabilité des données présente 3 opportunités pour les consommateurs de contenu digital : une réduction des switching costs et, par extension, des effets de lock-in. Également, la portabilité permet une libération de l'emprise des effets de réseaux en promouvant un libre arbitre dans le choix en produits ou services digitaux.

II. Réduction des switching costs

Dans un environnement digital soumis à bien des évolutions disruptives, il importe de prendre conscience des opportunités que représente le droit à la portabilité pour les consommateurs de contenu digital.

Auparavant, un utilisateur de plateforme quelconque désireux de basculer vers les services d'une plateforme concurrente, encourait des « switching costs » considérables afin de changer de prestataire de services. À savoir, les coûts de changement représentent « les coûts économiques et psychologiques associés au passage d'une alternative à une autre » (Jones & al., 2002). En pratique, les switching costs sont représentés par l'abandon de l'historique, des préférences et autres jeux d'information construits par l'utilisateur au fil du temps et dont la réutilisation sur une autre plateforme lui aurait été utile (Pernot, 2018).

Selon Engels, les switching costs sont particulièrement élevés au sein des réseaux sociaux. Bien qu'il soit possible de recevoir une copie des données, le format reste difficilement transférable vers un service concurrent ce qui rend la tâche chronophage et se traduit par des coûts de procédures élevés. Ainsi, la difficulté à transférer les contacts, messages, commentaires et photos vers d'autres réseaux sociaux, incite les utilisateurs à rejoindre le réseau social numéro un afin d'interagir avec un maximum d'individus (Engels, 2016).

En 2003, Burnhan, Frels et Mahajan proposent une typologie des coûts de changement en identifiant trois types de coûts distincts. En premier lieu, les coûts de procédures représentent le temps et les efforts investis dans la quête du changement de

fournisseur. Deuxièmement, les coûts financiers regroupent l'argent dépensé et devenu non récupérable lors de l'expérience avec le prestataire initial. Troisièmement, la perte d'identité suivant la rupture des liens émotionnels entre le client et la marque est représentée par les coûts relationnels (Burnham & al., 2003).

Ainsi, aussi longtemps que les switching costs excèderont les avantages retirés de l'utilisation d'une plateforme concurrente, la fidélité du consommateur restera l'optimum décisionnel bien que le niveau de satisfaction envers le service ne soit pas maximal (Manant & al., 2018). Or, la plupart des outils digitaux amenés par la révolution technologique visent justement à réduire les coûts de changements (Tucker, 2019), si bien que Krämer et Stüdlein avancent que le droit à la portabilité des données instauré par le RGPD fait tendre les switching costs vers zéro (Krämer et Stüdlein, 2019).

L'industrie des logiciels est marquée par diverses tendances digitales facilitant le transfert des données. Premièrement, la désormais capacité de stocker les données sur le cloud rend facile le voyage des données entre différents appareils (Tucker, 2019). Deuxièmement, les stratégies de tarification des plateformes étant désormais majoritairement construites autour des abonnements et non plus basées sur l'achat définitif, il est devenu moins contraignant pour un utilisateur de changer de prestataire de services. Enfin, le transfert de données entre systèmes d'exploitation est également devenu aisé, en témoigne l'application d'Apple permettant de déplacer les messages, contacts, photos et e-mails enregistrés sous Androïd vers l'iOS (Tucker, 2019).

La perception des coûts de changement par les consommateurs influe sur leur manière de réagir aux expériences insatisfaisantes. Les efforts et la complexité de changer de prestataire ainsi que les coûts psychologiques liés à la rupture de l'attachement émotionnel envers l'entreprise influencent positivement les intentions et les comportements d'achats répétés (Bergel et Brock, 2018). Également, certains utilisateurs insatisfaits s'estimant limités dans leurs possibilités d'envisager un service alternatif laissent paraître une grande colère les menant jusqu'au bouche-à-oreille négatif. A contrario, les consommateurs satisfaits, bien qu'ayant conscience de coûts de changement importants, s'adonnent volontiers à un bouche-à-oreille positif (Bergel et Brock, 2018).

Ainsi, nous en déduisons l'hypothèse suivante selon laquelle le droit à la portabilité est vu comme une aubaine par les consommateurs et qu'il est donc apprécié de ceux-ci (H1c). Cependant, avant de juger l'appréciation des consommateurs envers pareille prérogative, nous tenons à nous assurer que ce droit est d'une part compris (H1b) et que la conscience du recours à la portabilité est suffisamment élevée que pour l'exercer (H1a).

IIa. Réduction de l'effet de "lock-in"

Le marché ayant conscience d'un tel effet de verrouillage de la clientèle sur une plateforme initiale, le contexte était propice aux abus de positions dominantes comme une tarification plus élevée que la norme ou une réduction progressive de la qualité des services (Manant & al., 2018).

Le modèle des plateformes étant basé sur la génération d'informations de profil, de commentaires et d'évaluations par ses utilisateurs, les difficultés à transférer ces données vers d'autres systèmes accentuaient jusqu'alors la captivité des utilisateurs (Lambrecht, 2016). Une telle manoeuvre correspond à l'effet de "lock-in", défini comme étant "une stratégie par laquelle un fournisseur maintient une clientèle captive en faisant en sorte que les coûts de changements soient élevés" (Lambrecht, 2016).

Grâce aux données interopérables entre responsables de traitement, le droit à la portabilité des données amoindrit le coût de changement pour justifier le passage à la concurrence ou à tout le moins la complémentarité entre services (Manant & al., 2018). L'article 20 du RGPD possède donc les mêmes propriétés qu'une loi antitrust, dans la mesure où le voyage des données prévient tout abus de pouvoir et offre aux consommateurs une ouverture à la concurrence en favorisant la quête d'une qualité de service supérieure (Manant & al., 2018).

III. Effet réseau

Selon Lynskey, l'industrie du digital étant soumise à des forces de monopolisation, les externalités de réseau représentent alors une menace quant au contrôle individuel des données personnelles (Lynskey, 2015). L'externalité de réseau ou encore effet de réseau est définie par Katz et Shapiro comme étant l'accroissement d'utilité pour un utilisateur en fonction du nombre d'adopteurs du produit ou service (Katz & Shapiro, 1994). Dans le même ordre d'idées, l'effet Mathieu stipule quant à lui que la popularité est attrayante (Merton, 1968).
Or, vu sous un autre angle, l'innovation, les acquisitions et les effets de réseaux liés à l'industrie digitale biaisent le libre choix en produits ou services des consommateurs et représentent donc une externalité négative (Lynskey, 2015).

Parallèlement, un marché caractérisé par des externalités de réseau peut rapidement revêtir la forme d'un marché "winner-takes-all" ce qui n'est pas toujours désirable en termes de bien-être sociétal (Teng & al., 2006). Afin de répondre à cette externalité négative, la portabilité des données permet aux individus de s'approprier les avantages de la valeur créée par leurs données personnelles en les réutilisant auprès d'une autre plateforme. (European Data Protection Supervisor, 2015). Selon Kamleitner et Mitchell, la visualisation des flux de données pourrait aider les consommateurs à mieux comprendre ce qu'il advient des données après que le consentement initial soit donné (Kamleitner & Mitchell, 2018).

De son côté, Tucker avance que les effets de réseau basés sur les données de l'ère digitale pourraient être plus faibles et moins stables que précédemment imaginés (Tucker, 2019). D'une part, les externalités de réseau ont la capacité de déstabiliser le pouvoir de marché. En effet, à l'instar de l'effondrement du réseau social MySpace, les effets de réseau sont tout autant responsables de la croissance des plateformes que de leur déclin (Tucker, 2019). Deuxièmement, de par leur nature, les effets de réseau peuvent être très localisés et ne sont donc pas généralisables à toutes les plateformes. De fait, selon Tucker, l'utilisateur moyen de Dropbox par exemple ou d'un autre système de transfert de fichiers, est insensible au nombre total d'utilisateurs de la plateforme, pour lui seul compte l'inscription des collaborateurs avec qui il compte partager des fichiers. Enfin, en contexte numérique, les utilisateurs sont souvent favorables à une communauté restreinte soit parce qu'ils jugent

certaines personnes désagréables ou soit parce qu'ils tiennent tout simplement à leur vie privée (Tucker, 2019).

IV. Points d'attention pour les consommateurs comme entreprises

Le groupe de travail "article 29", qui est un organe consultatif européen indépendant, souligne la présence de deux risques majeurs émanant de l'opération de transfert de données personnelles. Premièrement, étant donné que la portabilité vise à extraire les données personnelles du système d'information, le transfert des données est alors vulnérable aux fuites de données (Article 29 Working Party, 2016).

Deuxièmement, en récupérant leurs données personnelles à partir d'un service en ligne, les utilisateurs courent le risque de stocker leurs renseignements dans un système encore moins sécurisé que celui fourni par le service. Dès lors, le responsable de traitement, en bon père de famille, pourrait émettre des recommandations quant aux formats adéquats et mesures de cryptage à adopter par les utilisateurs afin de sécuriser leurs données (Article 29 Working Party, 2016).

Chapitre 2 : Le droit à la rectification des données

Cette fois, la rectification des données est source d'avantages, tant pour les détenteurs de données que pour les consommateurs.

I. Énoncé du droit

Dès l'instant où la personne concernée remarque que les données personnelles conservées à son égard ont un caractère inexact ou lacunaire, une demande de correction ou de complétion des renseignements personnels peut être introduite auprès du responsable de traitement (Article 16, RGPD).

II. Types de données erronées

Les anomalies dans les données collectées comme les valeurs manquantes, inexactes ou obsolètes, peuvent nuire aux efforts de marketing en présentant les consommateurs sous un profil de préférences biaisé (Even & al., 2010).

L'extraction des noms aux fins de marketing ciblé constitue la principale utilisation opérationnelle des données. À cet égard, les problèmes de qualité d'une base de données de marketing peuvent être évalués en fonction du fait qu'une communication financièrement désirable n'atteint pas le nom destiné ou, alternativement, qu'une communication est gaspillée sur un nom financièrement indésirable (Courtheoux, 2003). En particulier, les communications hautement personnalisées sont très sensibles financièrement aux inexactitudes et aux manquements figurant dans certains champs de données (Courtheoux, 2003).

En 2013, la société américaine Acxiom collectant pour fins de marketing les données de 190 millions de consommateurs, a mis à disposition le site internet AboutTheData.com à la suite d'un appel à la transparence des défenseurs de la vie privée. Depuis lors les voix s'élèvent pour souligner au combien les données conservées par les data brokers peuvent être incohérentes (Hicken, 2013).

Ainsi, pour le compte de la rubrique économique de CNN, une journaliste fut stupéfaite de découvrir que son profil digital revendu aux entreprises mentionnait qu'elle était âgée de 26 ans et maman de deux adolescents, ce qui est biologiquement improbable (Hicken, 2013). De la même manière, un investigateur de l'agence de presse Reuters se prêta à l'expérience et découvrit qu'il était âgé de 57 ans avec une épouse de 30 ans, une chaudière assez neuve, une télévision à l'ancienne, une voiture à essence et qu'il était sans enfants. Or, il s'avère que toutes ces informations, sans exception, étaient erronées (Bergin, 2018). Selon Acxiom, jusqu'à 30 % des renseignements figurant dans le profil d'une personne peuvent être erronés de par les diverses sources sur lesquelles l'information est basée, y compris des dossiers publics ou des sondages qui peuvent être inexacts ou périmés (Hicken, 2013).

Dans l'environnement du supply chain management, il est de première importance que les managers disposent d'une base de données à jour afin de prendre des décisions éclairées. Or, des erreurs dans les adresses de livraison des clients, émanant par exemple d'un changement de domicile non notifié, implique que des publicités ou que l'objet d'une commande ne parviennent jamais à leur véritable destinataire. L'entreprise est alors propice à des pertes de ventes potentielles et démontre un service à la clientèle de faible qualité (Hazen & al., 2014). Du point de vue du consommateur, la non-réception d'un service attendu est source de méfiance envers les pratiques commerciales de la firme (Grow, 2017). Par ailleurs, il devient difficile pour les consommateurs d'envisager une relation de confiance avec une entreprise qui se base sur des données erronées ou manquantes, ce qui peut aboutir sur un rejet de toutes initiatives reposant sur de telles données (Haug & al., 2011).

Ainsi, nous en déduisons l'hypothèse suivante selon laquelle le droit à la rectification des données est vu comme une opportunité par les consommateurs afin de renouer leur confiance envers les pratiques commerciales. Sous H2c, la possibilité de mettre ses données à jour est appréciée des consommateurs. Cependant, avant d'estimer l'appréciation du droit à la rectification par les consommateurs, nous tenons à nous assurer que ce droit est d'une part compris (H2b), et que la conscience du recours à la rectification est suffisamment élevée que pour l'exercer (H2a).

III. Amélioration de la qualité des données

Le développement des technologies de l'internet génère un flux exponentiel de données, si bien que leur volume actuel a dépassé les capacités de traitement des systèmes d'exploration de données (Garcia-Gil & al., 2019). L'inconvénient majeur que pose l'ère du Big data dans la gestion d'une vaste quantité d'informations est la présence de "noise" dans un ensemble de données. Provenant de l'anglais et entendu au sens de nuisance, le noise se réfère aux données erronées, manquantes ou incomplètes rallongeant le temps de calcul pour une extraction de valeur insuffisante (Garcia-Gil & al., 2019).

En 2003, Brown et Kros relèvent trois raisons principales pour lesquelles une incohérence au niveau des données est susceptible de se produire (Brown et Kros, 2003). La première raison est à relier aux facteurs de procédures à l'instar d'erreurs humaines fréquemment encourues dans la saisie des données. Deuxièmement, l'origine de données manquantes peut se trouver dans le refus de répondre à certaines questions perçues comme offensantes ou sensibles sur le plan personnel. Par exemple, les questions liées au niveau d'éducation, au revenu, à l'âge ou encore au poids génèrent potentiellement une absence de réponse de par leur intrusivité. Enfin, les réponses inapplicables ont lieu lorsque la particularité du répondant ne lui permet pas de répondre à une question qui concerne d'autres caractéristiques que celles dont il dispose (Brown et Kros, 2003).

L'intérêt particulier du Smart data est qu'il ne s'arrête pas au modèle des "3V" longuement suggéré par le Big data (volume, variété et vélocité). Effectivement, de nos jours un tel modèle semble dépassé étant donné que ces 3V ne se limitent qu'à la génération et au stockage de renseignements (Bastin & Tubaro, 2018). De son côté, le Smart data se concentre sur la pertinence des données plutôt que sur leur abondance. Ainsi, afin de filtrer les incohérences constituant un même dataset, deux nouvelles dimensions viennent former un modèle à "5V" : la véracité et la valeur.

En comparaison avec les produits manufacturés de luxe, une qualité supérieure des données, considérées ici comme des produits virtuels, est peu onéreuse à atteindre. De fait, le coût des dépenses et des efforts gaspillés, lié au manque de considération pour un contrôle de la qualité des données, excède largement les coûts pour obtenir et maintenir des données pertinentes. Dans un univers marketing reposant sur les bases de données, les coûts associés à une sélection erronée de noms lors d'une campagne de marketing ciblée dépassent les coûts d'un programme de Data Quality Management (DQM) (Courtheoux, 2003).

Supposons le parcours d'un en-cours défectueux le long d'une chaîne de production. Chaque étape supplémentaire de la chaîne, de par les investissements encourus, ne fait qu'accroître les dommages collatéraux de la défaillance initiale. La gestion d'une base de données fonctionne de manière similaire (Courtheoux, 2003).

Dès lors, en exerçant son droit à la rectification des données, la personne concernée alimente l'efficience du Smart data. De fait, pour qu'une donnée soit considérée comme intelligente, elle doit être précise, activable et agile. À savoir, la correction améliore la précision de l'information, est exploitable pour suivre les objectifs d'une entreprise et enfin, est ajustable en temps réel (Garcia-Gil & al., 2019).

IV. Customer relationship management

L'utilisation de techniques de "data mining", entendues au sens de modèles et règles permettant d'extraire de l'information pertinente d'une masse de données, se dévoile être un précieux allié dans la quête d'une meilleure gestion de la relation client (Guo & Qin, 2017). Cependant, le récent afflux massif d'informations contenues dans des bases de données bien souvent incohérentes est source de préoccupations pour les entreprises. En effet, la recherche démontre que les professionnels du marketing sont peu désireux d'exploiter leurs bases de données sans avoir une totale confiance envers la qualité des données collectées. Alors, l'identification des procédés permettant un meilleur contrôle de la qualité des données, en vue de mieux comprendre la clientèle, vire à l'obsession pour les marketers (Zahay & al., 2012).

Le customer relationship management est une approche stratégique visant à créer de la valeur pour les actionnaires en développant une relation appropriée avec les consommateurs clés (Payne et Frow, 2005). En outre, le CRM offre de meilleures possibilités dans l'exploitation des données afin de mieux comprendre les clients et de créer de la valeur avec eux (Payne et Frow, 2005). L'objectif des solutions de CRM est d'augmenter la satisfaction de la clientèle en vue de la réalisation des objectifs d'une organisation (Chiranjeevi & al., 2018).

Dans leur étude, Even et al. illustrent un cas d'application du customer relationship management en analysant la qualité d'une base de données utilisée dans la gestion des relations entre une université et ses alumni (Even & al., 2010). Pour chaque alumnus qualifié de prospect, c'est-à-dire ayant été donateur par le passé ou dont le potentiel laisse présager un acte similaire, un membre du personnel est assigné au maintien de la relation avec l'université. L'analyse de la base de données révèle que 84% des profils de prospects ont des valeurs manquantes et 22% n'ont pas mis à jour leurs données au cours des 5 dernières

années. Dès lors, une telle constatation implique que des éléments cruciaux dans l'optimisation du CRM manquent à l'appel, en témoigne l'absence fréquente de notification lors d'un changement de revenu, d'adresse ou de statut marital (Even & al., 2010).

L'impact des données de mauvaise qualité est ressenti négativement des deux côtés de la relation établie par le customer relationship management. En effet, on observe une baisse de la satisfaction des consommateurs, mais aussi une inefficacité dans les procédés de prise de décision, une baisse de la performance ainsi qu'une dégradation de la satisfaction retirée par les employés (Haug & al., 2011).

Les effets de gestion de la relation client ont un impact positif sur la satisfaction des consommateurs. Si une organisation a une bonne stratégie CRM, alors la satisfaction du client sera automatiquement augmentée. À l'inverse, une mauvaise implémentation CRM se traduira par l'insatisfaction des consommateurs (Rahman, 2015). Au cours des dernières années, les organisations ont réalisé que le facteur clé de succès n'est pas d'obtenir une conversion unique, mais bien de bâtir une relation de long terme avec leurs clients (Rahman, 2015).

Pour conclure le présent chapitre, il semble que entreprises comme consommateurs peuvent juger utile l'exercice du droit à la rectification en tant que catalyseur de la fiabilité des données utilisées par les outils marketing des firmes à destination de leurs clients actuels ou potentiels.

V. Points d'attention pour les entreprises

L'émergence des techniques de marketing basées sur l'analyse de données en temps réel est capable d'augmenter le bien-être du consommateur en rendant ses choix plus faciles. Néanmoins, le point de tension réside dans le fait que le data-driven marketing est aussi susceptible de détruire ce même bien-être en annihilant l'autonomie des décisions prises par les consommateurs (André & al., 2018).

Parallèlement, Jean-François Ouellet avance que la relation actuelle entre satisfaction et loyauté pour laquelle deux fois plus de satisfaction fait plus que doubler la probabilité de loyauté à la marque, est vouée à s'inverser. Selon lui, la surabondance de modèles d'affaires transformant le consommateur en client automatique entraînera le déclin de la satisfaction client et de l'intérêt qu'ont les entreprises à la stimuler. L'accélération des innovations basées sur l'intelligence artificielle, bien intégrée dans la conscience collective des consommateurs, risque de faire chuter la satisfaction des clients envers les entreprises en marge du mouvement (Ouellet, 2018).

Chapitre 3 : Le droit à l'effacement des données

0. Contexte

La volonté première de construire un cadre juridique autour du droit à l'oubli numérique fait suite à une plainte déposée par un citoyen espagnol. En soumettant son nom au moteur de recherche Google, ce dernier a constaté un référencement d'hyperliens divulguant des informations litigieuses à son égard, portant ainsi préjudice à son capital image et au bon déroulement de ses affaires. Dans ce cadre, la Cour de Justice Européenne a accordé un droit à l'oubli numérique aux citoyens européens concernant les contenus identifiables à un tiers et dont la conservation au-delà de la durée nécessaire devient nuisible au respect de la vie privée (Simonnot, 2016).

I. Énoncé du droit

Ainsi, dans sa version finale inscrite dans le Règlement n° 2016/679 du Parlement européen (RGPD), « le droit à l'effacement des données » confère à la personne concernée le droit d'exiger (à titre d'obligation) du responsable de traitement, l'effacement des données qui lui sont identifiables, et ce dans les meilleurs délais (Article 17, RGPD).

II. Génération Z et vie privée en ligne

L'article 17 du RGPD nous rappelle un cas d'application précis où l'usage du droit à l'effacement se révèle particulièrement utile. Dans le cadre de la société de l'information, des données prélevées sur une personne encore mineure au moment de la collecte justifient le recours à l'effacement (Article 17, RGPD). Dès lors, une population semble particulièrement concernée par l'évocation d'un tel droit, celle de la génération "Z". La génération Z regroupe les personnes nées à partir de 1995, est très instruite, à la pointe de la technologie et créative (Herrando & al., 2019). Cette génération est la première qui, née dans un monde digital, est en mesure d'interagir virtuellement avec ses marques préférées (Priporas & al., 2017).

Tout comme les adultes, les enfants sont également dotés d'un pouvoir d'achat, conféré par l'argent de poche qu'ils reçoivent de leurs parents et peuvent donc également être qualifiés de consommateurs (Bartoli, 2009). Le pouvoir d'achat des adolescents a triplé depuis les années 1990 et les dépenses annuelles mondiales intervenant de leurs propres poches sont de l'ordre de 300 milliards de dollars (Nairn et Monkgol, 2007). De plus, les enfants sont une aide à la décision lorsque leurs parents envisagent des achats importants. Plus précisément, les jeunes consommateurs, moins averses au risque devant la nouveauté, sont particulièrement influents dans l'achat de produits technologiques pour lesquels leurs connaissances surpassent celles de leurs parents (Nairn et Monkgol, 2007). Ainsi, les publicités destinées au grand public ont la capacité d'éveiller tout autant l'attention des parents que celle de leurs enfants (Bartoli, 2009).

Les adolescents sont activement présents en ligne, et ce, à un âge de plus en plus jeune. À l'échelle mondiale, un internaute sur trois a moins de 18 ans (Macenaite et Kosta, 2017). Des études menées en Europe et en Amérique du Nord rapportent que les sites web majoritairement utilisés par les enfants, à savoir YouTube, Facebook et Google, mentionnent dans leurs conditions d'utilisation le refus de servir les moins de 13 ans. Pourtant, bon nombre des enfants compris dans cette tranche inférieure d'âge figurent parmi les utilisateurs actifs de ces plateformes. Par conséquent, les jeunes utilisateurs non autorisés sont exposés aux mêmes paramètres de confidentialité que les adultes sans discernement de leurs

caractéristiques comportementales propres comme l'impulsivité ou la volatilité émotionnelle (Macenaite et Kosta, 2017).

La différence entre adultes et adolescents dans la divulgation de données personnelles réside dans les différences de perception des finalités marketing du traitement des données. En particulier, les jeunes de 12 ans, aux portes de l'adolescence, ne possèdent pas encore les mêmes connaissances en marketing que les adultes et comprennent donc moins bien l'intention persuasive des messages publicitaires (Reijmersdal & al., 2017). De nos jours, les spécialistes du marketing en ligne ont incorporé des divertissements interactifs, tels que des jeux, des concours ou des tirages au sort sur leurs sites web afin d'attirer l'attention des adolescents. Ainsi, l'aspect ludique de cette forme de marketing adaptée aux plus jeunes est mis à profit pour capturer des renseignements personnels en détournant l'attention (Youn, 2005).

Youn rapporte en 2005 que la plupart des adolescents sont prêts à fournir leurs noms, données démographiques, renseignements sur leur mode de vie et adresses électroniques. Ils sont cependant très prudents en ce qui concerne la divulgation d'informations sur leurs parents et peu sont disposés à fournir leurs adresses postales (33%) ou leurs numéros de téléphone (20%) (Youn, 2005). Une autre étude menée par Turow proposait des résultats similaires, les participants âgés entre 10 et 17 ans étaient bien plus disposés que les adultes à partager des informations personnelles aux "online marketers". En outre, la propension des mineurs à échanger des renseignements sur eux-mêmes ou sur des membres de leurs familles est significativement plus élevée lorsqu'ils se voient offrir une récompense en échange de divulgation (Turow, 2001).

Selon Milne et Gordon, lorsqu'un gain économique ou social découlant de la divulgation de données personnelles est plus important que la perte de vie privée, alors les consommateurs ont plus d'incitations à communiquer leurs données (Milne & Gordon, 1993). Ainsi, on s'attend à ce que la divulgation volontaire des adolescents soit influencée par les avantages futurs qu'ils en retireront (Youn, 2005). En conséquence, si une marque veut bénéficier d'un avantage concurrentiel auprès des jeunes, la preuve d'une utilisation adéquate des données au regard des finalités commerciales reste le meilleur chemin à suivre.

Dès lors, nous en déduisons l'hypothèse selon laquelle les consommateurs apprécieraient d'effacer des données jadis collectées alors que leur maturité n'était pas suffisante que pour saisir les implications commerciales d'un partage de données (H3c). Cependant, avant de juger l'appréciation des consommateurs envers le droit à l'effacement, nous tenons à nous assurer que ce droit est d'une part compris (H3b), et que la conscience du recours à l'effacement est suffisamment élevée que pour être exercé (H3a).

III. Contexte n°2

Auparavant, le concept de personal branding était réservé aux célébrités ainsi qu'aux leaders économiques et politiques. Cependant, l'émergence des outils en ligne a rendu possible la gestion d'une image de marque pour le commun des mortels (Labrecque & al., 2011). En 1997, Tom Peters, le père fondateur de l'auto-branding avance que toute personne est en mesure de devenir sa propre marque et de pouvoir la gérer comme un marketer. À l'ère du digital, le personal branding implique la création et l'entretien de profils sur les réseaux sociaux, pages internet et blogs personnels. En outre, l'adoption de stratégies SEO facilite l'accès d'autrui vers les informations propres à d'autres internautes (Labrecque & al., 2011).

IV. Personal Branding

Selon Shepherd, le marketing de soi regroupe les activités multiples habituellement entreprises par les individus dans l'optique de décrocher un emploi satisfaisant. Néanmoins, le personal branding est également utilisé pour différentes raisons sociales comme la construction d'amitiés, la rencontre amoureuse ou encore l'expression de soi (Shepherd, 2005). En fait, en construisant une identité de marque tout en communiquant son positionnement au marché, le personal branding est similaire au product branding (Labrecque & al., 2011).

Parallèlement, on observe une tendance des employeurs à rechercher, sur les réseaux sociaux, des informations ayant une incidence sur la sélection des candidats à l'embauche. Plus connues sous le nom de "Cyber-vetting", ces pratiques sont appréciées par les recruteurs puisque le manque de contrôle des données propagées en ligne permet de dévoiler la réelle identité des candidats. Effectivement, les employeurs parviennent alors à acquérir des renseignements que les candidats n'avaient peut-être pas l'intention de partager dans d'autres circonstances (Berkelaar & al., 2015).

Bien que les internautes s'essayent à la gestion des informations en ligne, des fragments résiduels de données peuvent subsister après les tentatives de suppression. En l'occurrence, il arrive que la source du contenu indésirable en refuse la suppression ou que le contenu soit diffusé plus loin que prévu étant donné la sous-estimation de l'étendue des réseaux (Berkelaar & al., 2015). D'autre part, lorsque le profil Facebook du candidat n'est pas ouvert au public, la liste d'amis reste tout de même accessible aux recruteurs et s'avère être une mine d'or pour capter des indicateurs de personnalité. La probabilité est élevée que certains amis n'aient pas leurs profils protégés, ce qui permet aux recruteurs de juger la personnalité par association avec le type d'amis dont le candidat dispose (Vatamanescu & Manuc, 2013).

En 2012, une enquête menée par Harris Interactive, questionnant plus de 7000 employeurs, a révélé que 2 entreprises sur 5 analysent les réseaux sociaux avant de prendre des décisions de recrutement (Vatamanescu & Manuc, 2013). De plus, une autre étude menée par Swallow auprès de 300 professionnels de l'embauche a montré que 69% des recruteurs ont rejeté un candidat sur base de contenus inappropriés retrouvés sur son profil virtuel (Suen, 2018). De la même manière, 29% des chasseurs de têtes avouent engager sur base d'indicateurs de confiance découverts sur les réseaux sociaux comme une bonne personnalité, une gestion d'image professionnelle ou encore d'excellentes compétences en communication (Vatamanescu & Manuc, 2013).

Enfin, les postulants perçoivent les réseaux sociaux tel un environnement complètement séparé du monde professionnel. Dès lors, si les organisations continuent à baser leurs décisions professionnelles en explorant les réseaux sociaux, les candidats pourraient reconsidérer leur utilisation en adoptant un ton plus réservé avec leurs amis (Stoughton & al., 2015). Ainsi, le droit à l'effacement permet d'appliquer les codes du personal branding en demandant la suppression de contenus inappropriés, directement auprès du réseau social, ce qui autorise alors les utilisateurs à se dévoiler sous leur meilleur jour auprès des employeurs.

V. Traitement illicite de données

Toujours selon l'article 17 du RGPD, les données à caractère personnel ayant fait l'objet d'un traitement illicite sont également concernées par le recours au droit à l'effacement.

C'est le cas notamment des données liées à l'affaire Cambridge Analytica qui ont été utilisées bien au-delà des attentes ou des intentions des utilisateurs (Nature, 2018). De fait, Cambridge Analytica a obtenu l'accès à 320 000 profils d'utilisateurs Facebook ainsi qu'aux données de leurs amis via l'application "thisisyourdigitallife" développée par Aleksandr Kogan, psychologue de l'Université de Cambridge (Schneble & al., 2018). Bien que les 320 000 utilisateurs de Facebook aient donné leur consentement pour que l'application utilise leurs données et celles de leurs amis, ces derniers n'ont pas été invités à donner leur consentement et aucun n'a consenti à transmettre leurs données à Cambridge Analytica (Schneble & al., 2018).

Ce dont les utilisateurs ont parfois du mal à prendre conscience c'est qu'une fois mises en commun et traitées par des algorithmes, certaines données anodines ont la capacité de révéler des informations sensibles alors que leurs propriétaires s'attendaient à ce qu'elles restent confidentielles (Nature, 2018).

Avant que n'éclate le Cambridge Analytica gate, fortement médiatisé, la société souffrait déjà d'un déficit de confiance envers les données. Effectivement, une enquête menée par la Royal Statistical Society en 2014 a révélé que 32% des répondants avaient un faible niveau de confiance envers les entreprises de l'internet et que 54 % avaient peu confiance en une utilisation appropriée de leurs données personnelles. Des tendances similaires ont été constatées dans la majorité des autres institutions statistiques (Shah, 2017).

En outre, en 2016, Uber fut la cible de vol de renseignements personnels, notamment de numéros de sécurité sociale, affectant 57 millions de ses utilisateurs et près de 600 000 chauffeurs (Computer Fraud & Security, 2017).

La publication de données piratées étant assimilée à un traitement illicite, il a été constaté que de tels incidents réduisent la confiance des consommateurs ainsi que les intentions d'achats en ligne, particulièrement auprès des personnes plus âgées (Chakraborty & al., 2016).

Également, le manque de transparence, en particulier dans les jours suivant la violation de sécurité, est responsable d'une détérioration de la relation entre les sites de e-commerce et leurs clients (Chakraborty & al., 2016). Afin de répondre à pareille constatation, l'article 33 du RGPD exige du responsable du traitement la notification de la fuite de données à l'autorité de contrôle dans les 72 heures suivant la prise de conscience de l'incident. Quant à lui, l'article 34 du RGPD exige la communication de l'incident, dans les meilleurs délais, à la personne concernée par la violation de sécurité (Article 33 et 34, RGPD).

Par ailleurs, selon Papacharissi et Fernback, dans un monde virtuel où le droit à la vie privée et à la sécurité sont valorisés par les utilisateurs, ces derniers ne prennent paradoxalement pas le temps de poser des actions destinées à se protéger. Ainsi, la lecture des conditions générales ou encore la désactivation des cookies sont des pratiques de sécurité sous-employées bien que la conscience de leur efficacité soit collectivement intégrée (Papacharissi et Fernback, 2005).

Enfin, la perte financière pour les entreprises victimes d'un accès non autorisé aux informations confidentielles est considérable. Effectivement, des études ont mis en évidence une chute immédiate de 5,6% du prix des actions suite à une brèche de sécurité (Curtis & al., 2018).

Chapitre 4 : Le droit d'accès à l'information

I. Énoncé du droit

Les articles 13 et 14 du RGPD stipulent que les responsables du traitement doivent fournir à la personne concernée les informations nécessaires sur la procédure de traitement et faire preuve de transparence quant à l'utilisation des données personnelles (Article 13 et 14, RGPD).

L'article 15 du RGPD prévoit que la personne concernée a le droit d'accéder aux données à caractère personnel ainsi qu'à certaines informations supplémentaires telles que les finalités du traitement et la période de conservation (Article 15, RGPD).

II. Marketing de label

Il y a asymétrie d'information car les utilisateurs en savent moins que le responsable de traitement sur le respect du code de conduite dans la gestion des données. Dès lors, dans la mesure où il reste difficile pour un utilisateur d'évaluer la qualité et l'éthique du traitement à l'avance, la protection des données possède les mêmes caractéristiques qu'un bien de confiance. En économie, un bien de confiance est un produit ou service dont les attributs intéressent les consommateurs, mais sont inobservables avant ou même après la consommation (Baksi & al., 2017). Au regard de la thématique de recherche, il serait intéressant de constater de quelle manière la visibilité d'un label "GDPR compliant" contribue à la confiance des consommateurs envers un responsable de traitement (H4c).

Dans bien des cas, l'asymétrie d'information peut être corrigée par des autorités reconnues qui attestent de la qualité d'un produit après inspection et délivrent ensuite un label reconnaissable (Bonroy et Constantos, 2008). Ainsi, l'article 43 du RGPD encourage fortement une certification volontaire des responsables de traitement par les autorités de contrôle ou par les organismes nationaux d'accréditation (Article 43, RGPD).

La littérature contemporaine ne s'est encore que peu intéressée aux perceptions des consommateurs à la vue d'un label garantissant la protection des données sur la toile. Néanmoins, les découvertes de Miyazaki et Krishnamurthy en 2002 suggèrent que les personnes averses au shopping en ligne étaient plus aptes à divulguer leurs informations personnelles à la vue de labels assurant la protection de leurs données (Miyazaki et Krishnamurthy, 2002).

D'autres recherches mettent en exergue le fait qu'une majorité de consommateurs, précisément 57% d'entre eux, assimilent faussement la présence d'une politique de confidentialité à une absence de collecte de données personnelles ou de partage de celles-ci à d'autres entités (Rifon & al., 2005). En outre, en se basant sur des connaissances erronées ou peu suffisantes en matière de pratiques de traitement de l'information, les consommateurs adoptent des comportements sur internet qui sont contre-productifs au label. Par conséquent,

les consommateurs ignorent le contenu des politiques de confidentialité en faisant le raccourci selon lequel leur vie privée est de toute façon protégée par la présence du label. Alors, sans même comprendre le sens de la politique de confidentialité, le label n'est qu'une illusion que la vie privée des internautes est protégée (Rifon & al., 2005). La constatation de cet élément théorique nous dévoile l'intérêt de vérifier que la signification du label soit comprise par les internautes (H4b).

Parallèlement, en lien avec le droit d'accès à l'information, les labels de protection de la vie privée augmentent le sentiment des consommateurs selon lequel le site internet va communiquer sur les données recueillies, la manière de recueillir et à qui les données seront partagées (Rifon & al., 2005). Également, un label de protection des données peut être pensé comme une stratégie de co-branding dans laquelle un site web s'associe avec une autorité tierce reconnue afin de gagner la confiance des clients potentiels (Miyazaki et Krishnamurthy, 2002).

Ainsi, nous en déduisons l'hypothèse suivante selon laquelle l'existence du logo "GDPR compliant" augmente la propension des consommateurs à partager leurs informations personnelles (H4c). Cependant, avant de vérifier cette hypothèse, nous tenons à nous assurer que la signification du logo est comprise (H4b) et que l'existence du logo est suffisamment présente dans l'esprit du consommateur afin qu'il puisse partager ses données en tout état de cause (H4a).

Finalement, les labels encouragent la divulgation de renseignements auprès de deux types de consommateurs vulnérables : ceux qui s'inquiètent de la protection de la vie privée en ligne, mais ne savent pas comment se protéger et ceux qui savent comment se protéger, mais qui n'y prêtent pas attention (Larose et Rifon., 2007). Dès lors, en parallèle avec les recherches soulignées par Larose et Rifon, nous jugeons intéressant d'introduire une variable comportementale de réticence préalable au partage des données et de vérifier que l'existence du logo "GDPR compliant" génère un plus grand partage des informations personnelles auprès des réticents comparé aux non réticents (H4d).

III. Le commerce des data-brokers

À la lumière de l'article 15, les personnes concernées ont le droit d'être informées au sujet des "destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées" (Article 15, RGPD).

Parmi ces catégories de destinataires, on retrouve les "data-brokers", c'est-à-dire les organisations qui extraient, transforment, regroupent puis vendent les données à des entreprises de marketing qui utilisent l'information pour cibler directement les consommateurs (Yeh, 2018). Dans un monde virtuel dépourvu de limites, les courtiers en données numériques collectent quotidiennement des données démographiques, économiques, comportementales, religieuses ou sexuelles. En 2014, l'industrie du courtage numérique était déjà constituée de milliers d'entreprises de tailles variées, générant plus de 200 milliards de dollars de revenu annuel (Crain, 2018).

Le problème majeur de la relation entre data brokers et sociétés de marketing est que leurs opérations peuvent intervenir à l'insu du consommateur et sans son consentement. De fait, la majorité des citoyens n'est pas consciente de l'existence de cette relation et de son impact sur les transactions quotidiennes étant donné que les data brokers opèrent en arrière-plan. En conséquence, deux préoccupations principales émergent : la violation à la vie privée et la discrimination non désirée des consommateurs par les data brokers (Yeh, 2018).

Dès lors, l'appel à la transparence illustré par le droit d'accès à l'information, intervient dans un contexte de débat autour de la collecte excessive de données, qu'elle soit privée ou étatique. Dans le cas des data brokers, les partisans à la transparence soutiennent que les consommateurs ont un besoin d'accès à l'information sur les pratiques de collecte afin de prendre des décisions rationnelles concernant leurs données personnelles. En particulier, la négociation entre data brokers et consommateurs sur les manières de collecter l'information assurerait aux utilisateurs un meilleur contrôle de leurs données (Crain, 2018).

Ainsi, dans l'optique de mieux contrôler le sort qui advient aux données personnelles une fois partagées, nous déduisons l'hypothèse suivante selon laquelle les consommateurs apprécieraient d'accéder aux données collectées, conservées et traitées à leur égard (H5c).

Selon Hoy et Milne, l'utilisation des données par des sociétés tierces au-delà du but initial et les techniques de ciblage comportemental sont des sources de préoccupations pour les deux sexes, mais plus encore pour les femmes (Hoy et Milne, 2010).
Le type d'informations personnelles que les consommateurs sont disposés à partager avec les data brokers peut être classé dans l'ordre croissant suivant de réticence à divulguer le renseignement : nom, renseignements démographiques et géographiques, suivis de l'historique des achats, coordonnées de contact, historique de navigation en ligne, niveau de revenu, renseignements médicaux et financiers (Jai & al., 2016).

Enfin, l'engagement et l'adhésion à des programmes de fidélisation aux marques sont des indicateurs importants de la volonté des consommateurs à partager leurs renseignements personnels avec les data brokers. (Jai & al., 2016).

IV. Data protection officer

Afin de pouvoir exercer leur droit d'accès à l'information, les citoyens européens doivent être en mesure d'identifier un représentant ou un département au sein d'une organisation dont la mission est de répondre à toute requête relative aux données (L'Hoiry et Norris, 2015). À cet égard, l'article 13 du RGPD rend impérative la communication des coordonnées du responsable du traitement ou de l'officier à la protection des données aux personnes concernées (DPO) (Article 13, RGPD). En particulier, Cliza et Spataru avancent que l'adresse postale, le numéro de téléphone et l'adresse électronique constituent le minimum d'information facilitant la prise de contact avec le DPO. Également, la mise en place d'une hotline ou d'un formulaire de contact sont d'autres moyens de communication à prendre en compte (Cliza et Spataru, 2018).

Le data protection officer agit en tant qu'intermédiaire entre les parties prenantes en présence : les autorités de contrôle, les personnes concernées, les organismes publics et les

entreprises (Cliza et Spataru, 2018). Le DPO est donc la personne de contact des personnes concernées pour toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice de leurs droits dans le cadre du RGPD. À mi-chemin entre profil juridique, managérial et informatique, le data protection officer s'assure de l'implémentation adéquate du RGPD par les entreprises (Chirica, 2017).

Des stratégies permettant de garantir aux clients la facilité d'envoyer une requête de droit d'accès aux données doivent être continuellement élaborées par le délégué à la protection des données. Effectivement, en adoptant des pages web optimisées pour la navigation avec un contenu pertinent directement repérable, les organisations peuvent faciliter la prise de connaissance des politiques de confidentialité et des moyens d'exercer le droit d'accès (L'Hoiry et Norris, 2015). Par exemple, un bon indicateur du souci qu'ont les entreprises à assurer la visibilité du droit d'accès est le temps pris par les utilisateurs pour atteindre les liens relatifs à la protection de la vie privée. À cause d'un manque d'ergonomie au niveau de l'interface et d'une information utile noyée au milieu de contenus non pertinents, 39% des sites web nécessitent au moins 5 minutes de recherche avant de parvenir aux liens sur le respect de la vie privée (L'Hoiry et Norris, 2015).

Pour que les résidents européens puissent exercer leur droit d'accès à l'information, il est indispensable qu'ils soient conscients du type de données collectées, conservées et traitées à leur égard. En fait, sans être notifiés de l'étendue des pratiques de traitement suivant la signature d'un contrat commercial, les citoyens n'ont pas l'information nécessaire pour pouvoir exiger une divulgation complète des données en activant leur droit d'accès (L'Hoiry et Norris, 2015). Dès lors, avant même de juger l'appréciation des Européens envers le droit d'accès, nous tenons à nous assurer que ce droit est suffisamment compris (H5b) et connu (H5a) que pour être appliqué.

En 2015, une enquête à travers 10 pays européens a démontré que seule la moitié des sites web d'entreprises informait les citoyens quant aux catégories de données collectées. Par ailleurs, une inégalité géographique apparaît quant au partage de cette information (L'Hoiry et Norris, 2015). De fait, dans des pays tels que l'Allemagne, la Hongrie et le Royaume-Uni, une vaste majorité (94%, 90% et 88% respectivement) des entreprises consultées

conscientisent leurs utilisateurs à l'égard du type de données collectées. A contrario, les entreprises du Luxembourg ne dévoilent l'information que dans 25% des cas. Le constat est d'autant plus édifiant pour la Belgique, pays pour lequel aucune entreprise consultée ne partageait alors une telle information (L'Hoiry et Norris, 2015). À la conscience de telles observations, on comprend l'importance du data protection officer en tant qu'avocat des consommateurs, permettant l'optimisation de l'exercice des droits avancés par le RGPD.

V. Points d'attention pour les citoyens européens

D'un point de vue sécuritaire, l'accès aux données par les citoyens permet de vérifier que les données sont exactes et protégées afin d'assurer l'intégrité des données (Liu & al., 2005). Et pourtant, selon le secteur concerné, les citoyens ne sont pas logés à la même enseigne dans la mise en œuvre de l'accès aux données. Effectivement, une étude menée en Finlande, pour laquelle 41 requêtes d'accès ont été envoyées à divers responsables de traitement, a souligné que les organisations issues du secteur public répondaient mieux aux exigences du droit d'accès à l'information que les acteurs du privé (Raento, 2006).

Par ailleurs, pour les cas où l'accès à la copie des données révélait des informations incomplètes, les données manquantes étaient bien souvent d'ordre transactionnel.
Ainsi, commandes, factures, paiements et soldes sont fréquemment omis parmi les catégories de données dont le traitement est à mentionner aux consommateurs. À savoir, ces manquements proviendraient d'une mauvaise compréhension des responsables de traitement quant à l'étendue des données qualifiées comme personnelles, bien souvent restreintes aux informations générales comme le nom, l'adresse ou le type d'abonnement (Raento, 2006).

Chapitre 5 : Le droit d'opposition au traitement

I. Énoncé du droit

Les personnes concernées ont le droit de s'opposer à tout moment au traitement qu'un organisme exerce sur leurs données personnelles en vue de réaliser un objectif précis.
Mais, "les raisons tenant à la situation particulière" de la personne et qui justifient le recours à l'opposition, doivent être données sauf pour les cas de prospection commerciale pour lesquels aucune justification n'est nécessaire à l'application du droit (Article 21, RGPD).

II. Profilage et display advertising

Sous le régime de l'article 22 du RGPD, la personne concernée est en droit de s'opposer à toute décision entraînant des répercussions négatives à son égard et reposant exclusivement sur un traitement automatisé comme le profilage (Article 22, RGPD).

Dans l'environnement du e-commerce, le profilage est communément utilisé pour résumer les intérêts et préférences révélées par l'utilisateur lors de son activité en ligne (Trusov & al., 2016). Le profilage est l'outil du ciblage comportemental utilisé dans la personnalisation des publicités et des offres de produits afin d'en optimiser le taux de réponse (Trusov & al., 2016). Cependant, un premier inconvénient du profilage est l'intrusion dans les comportements posés par les internautes, ce qui menace le respect de la vie privée (Such & al., 2013).

Prenons l'exemple d'un commerçant en ligne étant parfaitement conscient d'une préférence plus grande pour un bien plutôt qu'un autre, le vendeur est alors en situation de pratiquer une discrimination tarifaire sur base de la propension à payer des consommateurs (Such & al., 2013). À titre d'illustration, en 2000, Amazon a reçu des réactions négatives de ses consommateurs suite à l'adoption d'une stratégie de tarification dynamique. De fait, l'entreprise américaine d'e-commerce facturait des prix différents pour un même DVD sur base des caractéristiques des consommateurs comme leurs achats précédents. La stratégie jusqu'alors gardée secrète par Amazon alimenta l'indignation des consommateurs, à un tel point que des excuses publiques furent présentées par le géant de l'e-commerce (Ferguson, 2014).

Par ailleurs, un second inconvénient du profilage tout aussi dangereux pour la vie privée en ligne est lié au concept de “poor judgment”. Selon ce principe, les clients sont évalués et traités suivant des décisions automatisées basées sur une information personnelle incomplète ou inexacte. Ainsi, la segmentation de la clientèle étant désormais automatisée par certaines entreprises, un client peut se voir exclure d’un service suite à une erreur d’appréciation dans le jugement automatisé des caractéristiques communes aux consommateurs (Such & al., 2013).

Parmi les méthodes de ciblage comportemental figure le display advertising, regroupant les publicités graphiques aux abords des contenus consultés par les internautes.
Le display advertising apparaît sous des durées, animations et formats variés à l’instar d’affichages en bannières, gratte-ciels ou fonds d’écran. Bien que les publicités graphiques soient susceptibles d'apparaître sur tout type de sites internet, on constate récemment une nette hausse de leur emploi sur les réseaux sociaux. Effectivement, les trois réseaux sociaux majeurs que sont Facebook, Twitter et LinkedIn représentent 30% des dépenses totales en display advertising au cours de l’année 2015 (Auschaitrakul et Mukherjee, 2017).

Sur les réseaux sociaux, un contenu publicitaire sur mesure agit sur les perceptions des consommateurs de deux manières contradictoires. De fait, la proximité avec les centres d’intérêt pourrait rendre la publicité attrayante aux yeux de l’utilisateur. Néanmoins, une forme de panique et de répulsivité à l’annonce pourrait aussi être exacerbée par la sensation d’intrusion dans la vie privée des utilisateurs (Tucker, 2014). Selon Doorn et Hoekstra, l'ajout d'informations d'identification personnelle ou de transaction à une annonce, au-delà de l’utilisation des données de navigation, augmente le sentiment d'intrusion et résulte en une baisse des intentions d’achats. Cependant, cet effet négatif peut être partiellement contrebalancé en présentant aux consommateurs une publicité qui correspond à leurs besoins (Doorn et Hoekstra, 2013). De manière similaire, Sheehan et Hoy démontrent l’intérêt d’investiguer sur le niveau optimal de personnalisation (Sheehan & Hoy, 2000).

En 2015, les recherches de Bleier et Eisenbeiss ont souligné que les annonceurs les plus fiables aux yeux des consommateurs augmentent la perception d'utilité pour une publicité proche des intérêts du consommateur sans pour autant susciter du rejet. Dans les cas où le contenu publicitaire est en phase avec les intérêts de l'internaute, mais que l'annonceur est de moins bonne crédibilité alors le sentiment de violation de la vie privée entraîne quant à lui un rejet élevé de l'annonce (Bleier et Eisenbeiss, 2015).

III. Marketing automation

La prospection est le processus qui consiste 1) à trouver des clients 2) prêts à générer un revenu net élevé pour une organisation (Gombeski & al., 2002). Suite à l'émergence de l'utilisation des données en tant qu' "input" à la prise de décision marketing, le terme de "Marketing automation" apparaît pour la première fois en 2001 et fait référence à l'art d'automatiser la prospection commerciale (Heimbach & al, 2015). Les campagnes de marketing automation, en réduisant le temps autrefois consacré à la répétition de tâches commerciales, sont d'une grande efficacité pour les équipes marketing qui observent un meilleur engagement de leurs clients tout en créant de nouvelles opportunités de revenus (Wilkey, 2012). Bien qu'au départ, le marketing automation était destiné à supporter les 4 activités du marketing mix, son application est désormais réduite à la tarification personnalisée en temps réel, à la promotion et à la compréhension du customer journey (Hinz & al., 2011).

Le marketing automation est souvent confondu avec des disciplines comme le Customer relationship management (CRM) ou encore l'e-mail marketing. En réalité, le marketing automation se situe un cran plus loin en utilisant de multiples sources de données, notamment d'utilisateurs inconnus, afin de concevoir une communication en temps réel à travers tous types de touchpoints : sites web, applications, e-mails,.. (Heimbach & al, 2015). En s'adressant aux clients potentiels avec du contenu et des offres personnalisées comme des coupons sur-mesure, les clients sont supposés montrer une participation accrue et payer davantage attention à la communication de la marque (Heimbach & al, 2015).

L'essence même des campagnes de marketing automation consiste en la distribution d'e-mails scénarisés à des intervalles préalablement définis. Le déclenchement d'une action entreprise par le consommateur génère l'envoi d'un scénario d'e-mail au détriment d'un autre, c'est pourquoi le marketing automation est également appelé "trigger marketing" (Wilkey, 2012). Parmi les scénarii communément envisagés par les marketers, le panier abandonné sur le site du détaillant en ligne, les anniversaires ou les fêtes annuelles constituent des moments propices au lancement d'une campagne automatisée. Or, d'autres occasions moins évidentes, mais tout aussi puissantes sont également exploitables, en témoignent les opportunités de "cross-selling", entendues au sens de ventes complémentaires. En fait, en ayant connaissance des produits achetés par les consommateurs, il est possible de rationnellement prédire d'autres articles pouvant compléter la satisfaction du même besoin initial (Wilkey, 2012).

Selon Akçura, Ozdemir et Altinkemer, les opportunités de ventes complémentaires augmentent le surplus du consommateur et les profits totaux tout en baissant les prix à condition que la collecte d'informations personnelles soit modérée (Akçura & al., 2009).
À l'inverse, lorsqu'une entreprise exploite abusivement les renseignements personnels sans plafonner les activités de cross-selling, le rejet de l'offre par les consommateurs est alors susceptible de faire chuter le profit de la firme (Akçura & al., 2009). Similairement, Srinivasan et Akçura soulignaient déjà en 2005 que, pour obtenir des informations personnelles tout en respectant l'intimité du client, l'entreprise doit s'engager dans la restriction de ses activités de cross-selling. Autrement, l'inquiétude quant à l'étendue des activités de cross-selling baisse les intentions des consommateurs à partager leurs données personnelles, ce qui se traduit par une baisse des revenus de cross-selling et in fine, une diminution du profit (Akçura et Srinivasan, 2005).

Ainsi, nous posons l'hypothèse pour laquelle, en cas d'un traitement abusif de l'information comme notamment des activités de cross-selling non plafonnées, le droit d'opposition au traitement des données est apprécié des consommateurs (H6c). Cependant, avant de juger l'appréciation de cet outil juridique par les consommateurs, nous tenons à vérifier que le droit est compris (H6b) et que les techniques de cross-selling sont suffisamment connues des consommateurs que pour pouvoir s'y opposer (H6a).

IV. Personnalisation des e-mails et click through rate

L'e-mail est le canal de marketing direct le plus rentable (Hartemo, 2016), son efficacité à acquérir de nouveaux clients est 40 fois plus grande que l'efficacité jointe de canaux comme Facebook ou Twitter. Paradoxalement, la performance et l'acceptation de l'e-mail marketing auprès des consommateurs sont en déclin suite à la prolifération de courriels commerciaux non sollicités et intrusifs (Hartemo, 2016). Sur les 210 milliards d'e-mails envoyés chaque jour, les SPAMS comptent pour 78%, dont 93 milliards d'entre eux parviennent tout de même à infiltrer les filtres antispam ainsi que les listes noires (Reimers & al., 2016). Face à ce problème impactant les résultats des entreprises comme le bien-être des internautes, les spécialistes du marketing affinent les populations cibles et deviennent plus attentifs à la fréquence, au moment et à la pertinence de l'e-mail publicitaire (Micheaux, 2011).

L'utilisation des données personnelles, même fondée sur le consentement des internautes, est susceptible de générer des réactions négatives dès lors que le consommateur prend conscience que son identité n'a plus de secret pour les entreprises (White & al., 2008). Le rejet du consommateur face à un degré inapproprié de personnalisation correspond au concept psychologique de "réactance" selon lequel l'individu se défend psychologiquement pour maintenir sa liberté d'action. De manière concrète, la réactance des utilisateurs s'exprime par une baisse des intentions de click through rate, c'est-à-dire de la volonté de cliquer pour découvrir le contenu de la sollicitation commerciale (White & al., 2008).

Dans leur étude, White et ses coauteurs démontrent qu'en l'absence de justification explicite sur le lien entre la donnée tangible collectée et l'offre promotionnelle, la réactance augmente et les intentions de click through rate baissent. D'autre part, les résultats suggèrent que pour tirer profit de la personnalisation des e-mails, les entreprises doivent s'assurer de proposer un produit ou service dont l'utilité perçue supplante le coût psychologique d'un degré de personnalisation inapproprié. En effet, les consommateurs sont généralement disposés à supporter des coûts plus élevés pour acquérir des biens leur apportant plus de bénéfices (White & al., 2008).

Selon Merisavo et Raulas, l'envoi répété d'e-mails commerciaux est nécessaire au maintien et à la fidélisation de la clientèle. Néanmoins, un excès dans les sollicitations commerciales pourrait éveiller des attitudes négatives sonnant le glas de la relation entre l'entreprise et sa clientèle (Merisavo et Raulas, 2004). Bien que 75% des consommateurs dégagent de la valeur de courriels émanant d'entreprises avec lesquelles ils font affaire, seulement 17% d'entre eux sont désireux de recevoir des courriels de marchands non connus (Wattal & al., 2012).

La recherche de Wattal et al. a exploré la réponse des consommateurs face à un e-mail publicitaire personnalisé, soit sur base des produits en lesquels ils ont exprimé un intérêt antérieur, soit sur base de l'usage du prénom en guise de salutations (Wattal & al., 2012). Les résultats soulignent que lorsque l'usage des informations aux fins de personnalisation n'est pas évident aux yeux des consommateurs, alors on constate un résultat positif en termes de click through rate. En revanche, la personnalisation de l'e-mail par le prénom entraîne quant à elle une réponse significativement négative du consommateur. Il est à noter que cet effet est réduit lorsque le consommateur a déjà réalisé des achats préalablement auprès de l'annonceur. Également, un niveau déjà élevé de l'activité du consommateur à l'instar de clics sur d'autres e-mails publicitaires ou même d'achats, est associé à une réponse moins négative aux salutations personnalisées (Wattal & al., 2012).

Enfin, le droit d'opposition semble ouvrir une opportunité pour les consommateurs irrités de constater un degré abusif de personnalisation ou subissant une fréquence de sollicitation excessive. En ce sens, il permet à la personne concernée de ne plus figurer parmi la base de prospection de l'annonceur ou de revenir sur sa décision de consentir au traitement de ses données.

V. Points d'attention pour les entreprises

Les courriels jamais ouverts sont en hausse considérable et les internautes ont de plus en plus tendance à limiter ou à interrompre tout contact commercial électronique. En 2002, une enquête avait révélé que 40% des répondants percevaient le courriel non sollicité comme étant le pire fléau de l'industrie des technologies de l'information (Xingan, 2006).

Chapitre 6 : Le droit de limitation au traitement

I. Énoncé du droit

La limitation du traitement de données personnelles impose la conservation des données personnelles par le responsable du traitement tout en demandant le gel temporaire de l'utilisation de certaines données (article 18, RGPD).

II. Le cyberbullying

Dans le cadre de contentieux comme la diffamation sur internet, dont les délais de prescription sont courts, la conservation de la donnée sensible par le responsable de traitement est utile en tant que preuve dans un procès intenté par la victime (CNIL, 2018).

Le harcèlement virtuel, de l'anglais "cyberbullying", est la diffusion immédiate et répétée par un individu isolé, de photos, numéros de téléphone, statuts et vidéos dont le relais au sein d'une communauté virtuelle nuit à l'intimité de la victime.

Par exemple, le harceleur publie une image provenant d'une capture d'écran, ou contre le gré de sa victime d'un rapport sexuel (Gozlan, 2018).

Également, le harceleur, en analysant sa victime, est en mesure de cerner un trait de caractère ou un trait physique dont il sait sciemment que la diffusion sur les réseaux sociaux se traduira en une humiliation publique. La problématique suit ici le principe de désintimité, à savoir l'appropriation désormais collective d'un élément que la victime aurait voulu garder exclusivement pour elle (Gozlan, 2018).

En comparaison avec le harcèlement traditionnel, le cyberbullying apparaît comme étant bien plus cruel que son homologue hors ligne. En effet, de par leur nature, les agissements en ligne ont la capacité d'être plus intenses, fréquents, imprévisibles et difficiles à interrompre (Sabella & al., 2013). De plus, à la différence avec le harcèlement traditionnel, les harceleurs virtuels ne sont pas limités par l'espace ou par le temps. L'humiliation est d'autant plus facile à mettre en place si l'auteur des faits est couvert par l'anonymat, lui laissant le libre choix d'attaquer où il veut et quand il le souhaite. Avec l'apparition des

technologies de l'information et de la communication, les pensées malveillantes peuvent être propagées instantanément, à ceci près, que l'audience est cette fois bien plus large (Sabella & al., 2013). Par ailleurs, le cyberharceleur ne voit pas la réaction de sa victime, ce qui, dans le harcèlement traditionnel, lui aurait peut-être procuré une empathie freinant d'autres intimidations (Kowalski & al., 2014).

Dans une étude menée en 2009 par Vandebosch et Van Cleemput auprès de 2052 étudiants flamands âgés de 12 à 18 ans, 11 % des répondants ont affirmé avoir été la cible de harcèlement virtuel et 18% ont affirmé en avoir été les auteurs. La majorité des répondants (63,8%) a affirmé qu'il s'agissait d'un problème préoccupant (Vandebosch et Van Cleemput, 2009). Parmi les agissements perçus comme étant les plus nuisibles, on retrouve des pratiques liées à l'intrusion dans la sphère privée dont le transfert à une large audience est source d'inquiétudes pour la victime. Ainsi, les pratiques pouvant impacter les personnes concernées de manière grave sont le vol de renseignements personnels sur ordinateur (73%), la diffusion d'informations privées ou protégées sur internet (72%) ou encore la propagation de rumeurs par e-mail ou par téléphone (62%) (Vandebosch et Van Cleemput, 2009).

L'influence d'un épisode de harcèlement virtuel sur la perception des utilisateurs quant à l'utilité et la satisfaction retirée des plateformes des TIC fut déjà l'objet d'explorations. Dans l'étude conjointe de Camacho, Hassanein et Head, 36% des répondants aux questions ouvertes mentionnent une perte d'intérêt et une réduction de l'usage de Facebook suite à un traumatisme de harcèlement sur le réseau social (Camacho & al., 2014). Le niveau de satisfaction des utilisateurs est affecté en proportion de la gravité du harcèlement vécu (Camacho & al., 2014). De surcroît, à la perte d'intérêt s'ajoute un manque de confiance des utilisateurs envers Facebook, justifiant l'utilisation de réseaux sociaux alternatifs. Dès lors, il est légitime de poser la question de la réactivité et de la gestion optimale des entreprises des TIC face à des situations de cyberbullying (Camacho & al., 2014).

Ainsi, nous déduisons que l'insatisfaction des utilisateurs née d'un épisode de harcèlement peut être contrebalancée par l'hypothèse suivante : sous (H7c), les consommateurs apprécient la conservation des preuves de harcèlement par un responsable du

traitement. Cependant, avant de vérifier l'appréciation du droit à la limitation par les consommateurs, nous tenons à vérifier que leur compréhension (H7b) et leur conscience du droit (H7a) soient suffisamment élevées que pour exercer l'action protectrice.

Chapitre 7 : Hypothèses à tester

- **H1a :** La proportion de connaissance du droit à la portabilité (pouvoir de transférer ses données vers un autre service numérique) est supérieure à 50%
  H1b : La compréhension de la portabilité est supérieure à 4 sur une échelle de 7
  H1c : L'appréciation de la portabilité est supérieure à 4 sur une échelle de 7

- **H2a :** La proportion de connaissance de la possibilité de mettre à jour ses données personnelles est supérieure à 50%
  H2b : La compréhension de la rectification est supérieure à 4 sur une échelle de 7
  H2c : L'appréciation de la possibilité de mettre à jour ses données personnelles est supérieure à 4 sur une échelle de 7

- **H3a :** La proportion de connaissance du droit à l'effacement (demander la suppression des données jadis collectées) est supérieure à 50%
  H3b : La compréhension de l'effacement est supérieure à 4 sur une échelle de 7
  H3c : L'appréciation de la possibilité d'effacer des données jadis collectées est supérieure à 4 sur une échelle de 7

- **H4a :** La proportion de connaissance de l'existence du label RGPD est supérieure à 50%
  H4b : La compréhension de la signification du label est supérieure à 4 sur une échelle de 7
  H4c : La propension à partager les informations personnelles en présence du label est supérieure à 4 sur une échelle de 7
  H4d : En présence du logo, les réticents partagent plus leurs données que les non réticents

- **H5a :** La proportion de connaissance du droit d'accès (accéder aux données détenues par un organisme) est supérieure à 50%

  H5b : La compréhension de l'accès aux données est supérieure à 4 sur une échelle de 7

  H5c : L'appréciation de l'accès aux données est supérieure à 4 sur une échelle de 7

- **H6a :** La proportion de connaissance des activités de cross-selling est supérieure à 50%

  H6b : La compréhension du droit de s'opposer au traitement de données personnelles en cas de cross-selling est supérieure à 4 sur une échelle de 7

  H6c : L'appréciation de l'opposition en cas de cross-selling est supérieure à 4 sur une échelle de 7

- **H7a :** La proportion de connaissance du droit de conserver les preuves de harcèlement (demander le gel temporaire de l'utilisation des données) est supérieure à 50%

  H7b : La compréhension de la limitation est supérieure à 4 sur une échelle de 7

  H7c : L'appréciation de la conservation des preuves de harcèlement est supérieure à 4 sur une échelle de 7

- Chaque hypothèse Hxa peut être démultipliée en une hypothèse Ha' vérifiant l'influence de l'âge, du sexe, du niveau d'éducation et de l'addiction au smartphone sur la connaissance de l'outil juridique en question.

- Chaque hypothèse Hxb peut être démultipliée en une hypothèse Hb' vérifiant l'influence de l'âge, du sexe, du niveau d'éducation et de l'addiction au smartphone sur la compréhension de l'outil juridique en question.

- Chaque hypothèse Hxc peut être démultipliée en une hypothèse Hc' vérifiant l'influence de l'âge, du sexe, du niveau d'éducation et de l'addiction au smartphone sur l'appréciation de l'outil juridique en question.

Partie 2 : Étude quantitative

Chapitre 1 : La méthodologie

Au cours de ce premier chapitre, nous aborderons les étapes nécessaires au bon déroulement de l'étude empirique. Le présent mémoire repose sur une recherche de type quantitative. La méthodologie évoquée ci-dessous reprend la méthode de collecte de données ainsi que la concordance entre les hypothèses à vérifier et les questions constituant le questionnaire. Également, nous mentionnons les outils statistiques employés au regard des hypothèses à tester.

I. Collecte des données

L'extraction des données indispensables à la réalisation de l'étude empirique s'est effectuée à partir d'un questionnaire de nature quantitative soumis à un échantillon mesuré (cf. Annexe n°2). À l'aide de l'application d'administration d'enquêtes "Google Forms", des échelles métriques validées par la communauté scientifique ont permis de jauger l'attitude des individus face à diverses affirmations. Le questionnaire fut partagé sur internet. La récolte de données ayant été échelonnée sur la première dizaine du mois de juillet 2019.

A. Questionnaire

L'emploi d'un questionnaire quantitatif est justifié par le besoin d'analyser un nombre relativement élevé de réponses nécessitant de pouvoir regrouper leurs résultats en une structure claire. Ainsi, l'utilisation d'une application telle que Google Forms, permettant la génération instantanée d'un panel de graphiques, répond au besoin de clarté à la rédaction avancé par Gordy Pleyers dans son cours "Analyser, prédire et optimiser les réactions des consommateurs "(Pleyers, 2018). L'enquête par internet s'avère être la méthode de collecte la plus rapide et permet un encodage immédiat dans les divers logiciels de traitement statistique (Lambin & de Moerloose, 2016). Également, la thématique de recherche impose que le questionnaire respecte la vie privée numérique des répondants. Dès lors, en introduction du

questionnaire nous mentionnons la garantie de l'anonymisation des réponses de par l'unique exploitation des résultats agrégés. Similairement, nous notifions aussi aux répondants que la finalité du traitement des réponses aura pour pure vocation la recherche scientifique et non un but commercial. Enfin, la confidentialité des réponses est respectée.

La version finale du questionnaire comprend 8 sections. Les 7 premières sections sont à chaque fois composées d'une question fermée dichotomique pour évaluer la connaissance de l'outil juridique et de deux questions fermées à choix multiple utilisant des échelles métriques et visant à juger la compréhension et l'appréciation du droit. La dernière section est particulièrement intéressante pour étudier l'effet des modalités et regroupe trois questions fermées dichotomiques pour définir deux attitudes comportementales et le genre du répondant ; deux questions fermées à choix multiple pour définir la catégorie d'âge et le niveau d'éducation ; une question facultative ouverte afin de recueillir le sentiment du répondant envers le questionnaire. À l'exception de la question ouverte, toutes les autres questions sont marquées par le caractère obligatoire de la réponse afin d'éviter que la base de données ne souffre de réponses manquantes au moment de l'analyse.

Avant de propager définitivement le questionnaire sur la toile, nous avons réalisé un prétest de celui-ci sur un nombre limité de répondants : 4 personnes de profils différents âgées de 20 ans à 55 ans. L'objectif était ici de nous assurer que les questions soient comprises par les répondants et que l'agencement de celles-ci soit optimal. À l'issue de la phase de prétest, la compréhension des questions fut confirmée alors que l'ergonomie du questionnaire fut remise en question. Ainsi, avant d'administrer le questionnaire de manière définitive, une dernière modification dans l'ordre d'apparition des questions fut nécessaire afin de ne pas influencer les autres questions par un effet de "contamination".

B. Échelles de mesure

Dans l'optique de construire un questionnaire pertinent, une échelle psychométrique particulière de renom au sein du monde académique fut utilisée tout au long de l'enquête. Pour chaque section concernée du questionnaire, les échelles de mesure suivaient un schéma similaire : évaluer le niveau de compréhension et d'appréciation des actions protectrices

proposées par le RGPD. Les échelles étaient toutes de type sémantique de Likert comportant 7 options de réponses allant d'une attitude extrême à une autre. L'échelle attitudinale de Likert permet ainsi aux répondants de donner leur degré d'accord ou de désaccord envers une affirmation (1= pas du tout d'accord ; 7= tout à fait d'accord). L'intérêt particulier de recourir à une échelle constituée d'un nombre impair de points est d'offrir aux répondants la capacité de nuancer leurs jugements sans les inciter à pencher vers un extrême au détriment d'un autre (Pleyers, 2018).

C. Échantillon

La version définitive du questionnaire fut propagée sur la toile par l'intermédiaire d'e-mails et de contacts sur le réseau social Facebook. De manière concrète, le sondage fut partagé à des connaissances aux profils différents, qui à leur tour ont diffusé le questionnaire à leurs proches, amis et familles. Ainsi, cette approche d'administration d'enquête revêt la forme de "boule de neige" et a permis la participation de répondants aux profils variés. Néanmoins, l'utilisation d'une telle technique de diffusion par internet est propice à un biais de représentativité puisque la population d'étude est limitée aux répondants qui possèdent ce média et en maîtrisent les rouages (Lambin & de Moerloose, 2016). Ainsi, d'un point de vue sociodémographique, la population d'étude exclut par exemple les personnes âgées désintéressées ou inaptes à l'utilisation d'internet. Également, les classes socio-économiques inférieures dont le revenu n'est pas suffisant que pour posséder des devises connectées à internet sont susceptibles d'être sous-représentées dans l'étude. Cependant, l'enquête par internet reste pertinente lorsqu'elle cible les internautes (Lambin & de Moerloose, 2016).

Dès lors, dans la mesure où le thème de recherche couvre principalement la protection et le contrôle de la vie numérique des internautes, nous jugeons pertinente la diffusion de l'enquête en "boule de neige" sur la toile.

II. Tableau de croisement Hypothèses - Questions

Dans cette section, nous estimons utile d'insérer une matrice de concordance entre les hypothèses à vérifier et les questions de l'enquête afin de nous assurer que chaque question soit "nécessaire et suffisante". L'intérêt d'employer cette matrice est double puisqu'elle permet également de "vérifier que la nature des échelles choisies (N=Nominale, O=Ordinale ou M=métrique) correspond bien au test futur envisagé" (Lambin & de Moerloose, 2016).

Questions Nature Hypothèses	Q1 (N)	Q2 (M)	Q3 (M)	Q4 (N)	Q5 (M)	Q6 (M)	Q7 (N)	Q8 (M)	Q9 (M)	Q10 (N)	Q11 (M)	Q12 (M)	Q13 (N)	Q14 (M)	Q15 (M)	Q16 (N)	Q17 (M)	Q18 (M)	Q19 (N)	Q20 (M)	Q21 (M)	Q22 âge (O)	Q23 éduc (O)	Q24 sexe (N)	Q25 accro (N)	Q26 réticence (N)
H1a	B																									
H1b		T																								
H1c			T																							
H2a				B																						
H2b					T																					
H2c						T																				
H3a							B																			
H3b								T																		
H3c									T																	
H4a										B																
H4b											T															
H4c												T														
H4d																										χ^2
H5a													B													
H5b														T												
H5c															T											
H6a																B										
H6b																	T									
H6c																		T								
H7a																			B							
H7b																				T						
H7c																					T					
Hxa'																						χ^2	χ^2	χ^2	χ^2	
Hxb'																						T	A	T	T	
Hxc'																						T	A	T	T	

Légende de la matrice : Outils statistiques : T= test T, B= test Binomial, A= Anova , χ^2= Chi-carré

Réutilisation de la variable associée

Chapitre 2 : Analyse des résultats

Au cours de ce chapitre, les résultats de la recherche empirique seront traités à l'aide de l'outil informatique d'exploitation de données " IBM SPSS Statistics 20".

I. Préparation des données

À la fin de l'enquête, nous avons préparé les données brutes avant d'entamer l'analyse statistique à proprement parler. Les données acquises auprès de nos 123 répondants furent exportées dans le logiciel SPSS Statistics 20. En premier lieu, l'affichage des réponses par heure étant peu nécessaire à l'analyse, nous avons supprimé la colonne horodateur fournie par défaut par l'application Google Forms. Deuxièmement, dans l'optique de faciliter la manipulation des données, nous avons simplifié le nom des variables dont la correspondance est disponible dans le dictionnaire des variables (cf. Annexe n°3). Également, afin de permettre au programme SPSS de procéder à l'analyse, nous avons mis à jour le type des variables en recodant les variables nominales en versions chiffrées. De manière connexe, une définition de l'ensemble des modalités est également à retrouver dans le dictionnaire des variables (cf. Annexe n°3). En explorant la base de données, nous observons que seuls 4,9% des répondants ont entre 10 et 20 ans et 8,1% ont entre 41 et 50 ans. Dès lors, nous décidons de regrouper l'âge en deux modalités : les 10-30 ans et les 31 ans et +. Enfin, à partir de l'analyse de fiabilité et de l'ACP, nous créons une variable agrégée évaluant la compréhension du RGPD et une autre variable agrégée évaluant l'appréciation du RGPD (cf. Annexe n°3).

II. Analyse descriptive de l'échantillon

L'échantillon final de l'étude empirique est de taille n=123 répondants. La répartition de l'échantillon selon le genre des répondants est la suivante : 52% de femmes et 48% d'hommes (cf. Annexe n°4). Le test de représentativité fourni ci-après par la figure 1 nous permet de souligner la répartition équitable de l'échantillon en fonction du genre.

Figure 1 : Test de la parité du genre des répondants

Nonparametric Tests

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The categories defined by Sexe = Masculin and Féminin occur with probabilities 0,5 and 0,5.	One-Sample Binomial Test	,718	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is ,05.

De plus, comme le démontre la figure 2, la distribution de l'échantillon selon le sexe suit une tendance similaire aux chiffres avancés par la banque de données mondiale. Effectivement, en 2018, la population mondiale est composée à 49,549% de femmes et à 50,451% d'hommes (World Bank Open Data, 2019).

Figure 2 : Test de similarité à la répartition mondiale du genre

Nonparametric Tests

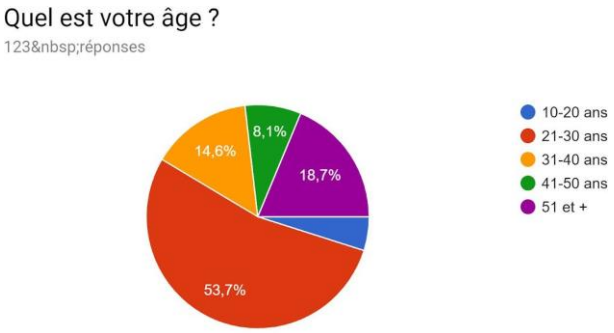
Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The categories defined by Sexe = Masculin and Féminin occur with probabilities 0,505 and 0,495.	One-Sample Binomial Test	,322	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is ,05.

En ce qui concerne la variable ordinale de l'âge, initialement subdivisée en cinq catégories d'âge, nous pouvons constater que 4,9% des répondants ont entre 10 et 20 ans, 53,7% ont entre 21 et 30 ans, 14,6% ont entre 31 et 40 ans, 8,1% ont entre 41 et 50 ans, enfin 18,7% des répondants ont 51 ans et plus. L'insertion d'un diagramme en secteurs permet ici une facilitation visuelle améliorant la compréhension de la répartition de l'échantillon.

Figure 3 : Répartition des répondants selon l'âge (source : notre enquête)



À la lecture de la figure 3, la majorité des participants a déclaré avoir entre 21 et 30 ans. La prise en considération d'une telle observation permet d'intégrer la présence d'un biais au déroulement de l'analyse. La surreprésentation des "21-30 ans" peut être expliquée par leur plus grande présence parmi les moyens d'administration de l'enquête.

Figure 4 : Répartition des répondants selon le niveau d'étude (source : notre enquête)

En observant la figure 4, une majorité (56,1%) des répondants est issue des études supérieures de niveau master ou similaire. Néanmoins, cette majorité est suivie de près par une bonne représentation des profils de bacheliers (37,4%). Le niveau d'instruction inférieur est quant à lui représenté par 6,6% de l'échantillon, ce pourcentage étant la somme des non-diplômés (3,3%) et des profils issus de l'enseignement primaire ou secondaire uniquement (3,3%). De prime abord, nous pouvons penser à une sous-représentation des profils les moins instruits (6,6%).

Néanmoins, ce dernier pourcentage reflète plutôt bien les dernières tendances en matière de diplômes, soulignées par l'Iweps qui n'est autre que l'autorité statistique de la Région wallonne. En effet, en Wallonie, en 2018, "13 % des personnes âgées de 25 ans et plus n'ont pas de diplômes ou au maximum un diplôme de l'enseignement primaire" (Dujardin, 2019). La figure 5 ci-dessous illustre l'hypothèse selon laquelle l'échantillon suit une proportion conjointe de 0.13 pour les faibles niveaux d'enseignement et nous ne sommes pas en mesure de rejeter cette hypothèse.

Figure 5 : Test de représentativité des faibles niveaux d'étude

```
*Nonparametric Tests: One Sample.
NPTESTS
  /ONESAMPLE TEST (Niveaudétude) CHISQUARE(EXPECTED=CUSTOM(CATEGORIES=Autre Primaire-secondaire  FREQUENCIES=8.0 8.0 ))
  /MISSING SCOPE=ANALYSIS USERMISSING=EXCLUDE
  /CRITERIA ALPHA=0.05 CILEVEL=95.
```

Nonparametric Tests

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The categories of Niveaudétude occur with the specified probabilities.	One-Sample Chi-Square Test	1,000	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is ,05.

Enfin, 54,5% des sondés ont indiqué être "accros" au smartphone (cf. Annexe n° 5). D'autre part, 74,8% (cf. Annexe n°6) des répondants avouent être habituellement réticents à l'idée de partager leurs informations personnelles.

III. Analyse de la fiabilité des échelles

Dans cette section, nous utiliserons le coefficient alpha également appelé alpha de Cronbach, en tant qu'indicateur de la fiabilité des échelles de mesure de compréhension et d'appréciation des actions protectrices du RGPD. Le seuil minimum acceptable pour la valeur du coefficient d'alpha doit être de 0.7 pour véritablement qualifier l'échelle de fiable. À l'inverse, un coefficient d'alpha d'une valeur inférieure à 0.5 indique une réelle incohérence interne de l'instrument d'évaluation et par conséquent un manque de fiabilité de l'échelle (Swaen, 2017).

- **Échelle de compréhension**

De l'analyse de fiabilité, avec un alpha de Cronbach de 0,75 (cf. Annexe n°7) qualifié comme un "bon" indicateur de fiabilité, car compris entre 0.7 et 0.8 (Swaen, 2017), nous déduisons que les questions telles que formulées permettent de définir une échelle évaluant la compréhension du RGPD comprenant 4 éléments (cf. figure 6) : la compréhension de la rectification, celle de l'effacement, celle de l'accès et celle de l'opposition mesurées chacune sur une échelle de Likert en 7 points. La valeur minimale pour cette échelle agrégée sera de 4 et la valeur maximale de 28. Les participants ont une moyenne de 23,07 (cf. Annexe n°8).
On peut donc conclure que les répondants comprennent en moyenne le RGPD.

Figure 6 : Échelle de compréhension du RGPD réduite à 4 éléments

Statistiques de total des éléments

	Moyenne de l'échelle en cas de suppression d'un élément	Variance de l'échelle en cas de suppression d'un élément	Corrélation complète des éléments corrigés	Carré de la corrélation multiple	Alpha de Cronbach en cas de suppression de l'élément
Comprehensionrectification	17,29	11,143	,611	,442	,649
Comprehensioneffacement	16,77	13,899	,509	,323	,715
Compréhensionacces	17,74	10,424	,587	,387	,665
Comprehensioncrossselling	17,39	11,994	,491	,266	,719

- **Échelle d'appréciation**

De l'analyse de fiabilité, avec un alpha de Cronbach de 0,54 (cf. Annexe n°9) considéré comme un indicateur "insuffisant" de fiabilité sans pour autant être rejeté, car compris entre 0.5 et 0.6 (Swaen, 2017), nous déduisons que les questions telles que formulées permettent de définir une échelle évaluant l'appréciation du RGPD comprenant 4 éléments

(cf. figure 7) : l'appréciation de l'effacement, celle de l'accès, celle de l'opposition et celle de la limitation mesurées chacune sur une échelle de Likert en 7 points. La valeur minimale pour cette échelle agrégée sera de 4 et la valeur maximale de 28. Les participants ont une moyenne de 25,75 (cf. Annexe n°10). On peut donc conclure que les répondants apprécient en moyenne le RGPD.

Figure 7 : Échelle d'appréciation du RGPD réduite à 4 éléments

Statistiques de total des éléments

	Moyenne de l'échelle en cas de suppression d'un élément	Variance de l'échelle en cas de suppression d'un élément	Corrélation complète des éléments corrigés	Carré de la corrélation multiple	Alpha de Cronbach en cas de suppression de l'élément
Appreciationeffacement	19,23	4,849	,463	,216	,377
Appreciationaccces	19,41	4,277	,340	,140	,476
Appreciationcrosssel ling	19,19	5,432	,268	,094	,524
Appreciationlimitatio n	19,41	5,212	,284	,091	,513

IV. Analyse en composantes principales

Dans l'optique de vérifier la validité des échelles de mesure, nous devons tenir compte des deux conditions de réalisation de l'Analyse en composantes principales (ACP). Tout d'abord, l'indice de Kaiser-Meyer-Olkin (KMO) doit avoir une valeur comprise entre 0.5 et 1 pour que l'analyse soit considérée comme pertinente (Swaen, 2017). Deuxièmement, la deuxième condition de réalisation de l'ACP exige que la p-value au test de sphéricité de Bartlett soit significative, c'est-à-dire que $\alpha < 0.05$. Autrement formulé, le test de Bartlett est utile pour examiner l'hypothèse selon laquelle les variables ne sont pas corrélées dans la

population. Dans les cas où la corrélation entre les facteurs n'est pas suffisante, aucune réduction de l'information n'est envisageable (Swaen, 2017).

Nous avons par la suite procédé à diverses analyses en composantes principales dont le but majeur est "d'identifier quelles variables ou quels items sont corrélés entre eux et pourraient dès lors être regroupés en un plus petit nombre de facteurs" (Lefèvre et Taverne, 2017). Par ailleurs, l'ACP est également un outil permettant de vérifier la validité des questionnaires en psychométrie (Lefèvre et Taverne, 2017).

- **Compréhension du RGPD**

Figure 8 : Indice KMO et test de Bartlett pour l'échelle de compréhension du RGPD

Indice de Kaiser-Meyer-Olkin pour la mesure de la qualité d'échantillonnage.		,680
Test de sphéricité de Bartlett	Khi-carré approx.	188,864
	ddl	21
	Signification	,000

Avec un KMO de 0,680 et une p-value au test de sphéricité de Bartlett significative (0,000) (cf. figure 8), les conditions de réalisation de l'ACP sont respectées.

Figure 9 : Rotation de la matrice des composantes[a] de compréhension

	Composante	
	1	2
Comprehensionrectification	,780	,165
Compréhensionacces	,780	,000
Comprehensioneffacement	,738	,106
Comprehensioncrossselling	,654	,140
Comprehensionlimitation	,469	,238
Comprehensionlogo	,010	,879
Comprehensionportabilite	,260	,688

Méthode d'extraction : Analyse en composantes principales.

Méthode de rotation : Varimax avec normalisation Kaiser.

a. Convergence de la rotation dans 3 itérations.

Les sept éléments évaluant la compréhension des outils juridiques peuvent être réduits en deux facteurs : le premier fortement corrélé avec les 4 éléments qui forment l'échelle globale de compréhension construite à partir de l'alpha de Cronbach en plus de la compréhension de la limitation puis le deuxième corrélé avec la compréhension du label et celle de la portabilité (cf. figure 9). En termes d'interprétation, étant donné que l'ACP regroupe les variables semblables entre elles, un répondant comprenant au moins l'un des 5 outils suivants (rectification, effacement, accès, opposition ou limitation) et l'un des 2 outils suivants (label ou portabilité) aura tendance à comprendre en moyenne le RGPD.

- **Appréciation du RGPD**

Figure 10 : Indice KMO et test de Bartlett pour l'échelle d'appréciation du RGPD

Indice de Kaiser-Meyer-Olkin pour la mesure de la qualité d'échantillonnage.		,648
Test de sphéricité de Bartlett	Khi-carré approx.	66,293
	ddl	21
	Signification	,000

Avec un KMO de 0,648 et une p-value au test de sphéricité de Bartlett significative (0,000) (cf. figure 10), les conditions de réalisation de l'ACP sont respectées.

Figure 11 : Rotation de la matrice des composantes[a] d'appréciation

	Composante	
	1	2
Appreciationeffacement	,745	,111
Appreciationcrossselling	,668	-,296
Appreciationaccces	,593	,316
Appreciationlimitation	,543	,124
Appreciationportabilite	-,206	,718
Appreciationrectification	,274	,649
Renforcementlogo	,146	,535

Méthode d'extraction : Analyse en composantes principales.

Méthode de rotation : Varimax avec normalisation Kaiser.

a. Convergence de la rotation dans 3 itérations.

Les sept éléments évaluant l'appréciation des outils juridiques peuvent être réduits en deux facteurs : le premier fortement corrélé avec les 4 éléments qui forment l'échelle globale d'appréciation construite à partir de l'alpha de Cronbach puis le deuxième corrélé avec l'appréciation de la portabilité, celle de la rectification et celle du renforcement par le label (cf. figure 11). En termes d'interprétation, étant donné que l'ACP regroupe les variables semblables entre elles, un répondant appréciant au moins l'un des 4 outils suivants (effacement, accès, opposition ou limitation) et l'un des 3 outils suivants (portabilité, rectification ou label) aura tendance à apprécier en moyenne le RGPD.

V. Vérification des hypothèses de l'étude

A. Hypothèses principales

- **H1a :** Connaissance du droit à la portabilité (Test binomial sur une proportion)

La p-value de 0,857/2 = 0,428 (cf. Annexe n°11), ne nous permet pas de rejeter l'hypothèse nulle d'infériorité des proportions à 50%. On ne peut pas conclure que plus de 50% des répondants connaissent le droit à la portabilité.

- **H1b :** Compréhension du droit à la portabilité (Test T pour la comparaison de moyenne d'un échantillon)

La p-value de 0,000/2 = 0 (cf. Annexe n°12), nous permet de rejeter l'hypothèse nulle d'infériorité de la moyenne à 4. Avec une moyenne de l'échelle de compréhension de la portabilité égale à 4,62 (cf. Annexe n°12), qui est supérieure à 4, on peut conclure que la portabilité est plutôt comprise des répondants. La conclusion étant nuancée par une valeur de 4,62 relativement proche du seuil neutre de 4.

- **H1c :** Appréciation du droit à la portabilité (Test T pour la comparaison de moyenne d'un échantillon)

Avec une p-value de 0,001/2 = 0,0005 (cf. Annexe n°13), nous ne rejetons pas l'hypothèse nulle d'infériorité de la moyenne à 4. Avec une moyenne de l'échelle

d'appréciation de la portabilité égale à 3,38 (cf. Annexe n°13), qui est inférieure à 4, on peut conclure que la portabilité n'est pas appréciée des répondants.

- **H2a :** Connaissance du droit à la mise à jour des données personnelles (Test binomial sur une proportion)

La p-value de 0,004/2 = 0,002 (cf. Annexe n°14), nous permet de rejeter l'hypothèse nulle d'infériorité des proportions à 50%. Avec une proportion observée de 63% (cf. Annexe n°14) des répondants connaissant le droit à la rectification, on peut conclure que le droit à la rectification est connu des répondants.

- **H2b :** Compréhension du droit à la rectification (Test T pour la comparaison de moyenne d'un échantillon)

La p-value de 0,000/2 = 0 (cf. Annexe n°15), nous permet de rejeter l'hypothèse nulle d'infériorité de la moyenne à 4. Avec une moyenne de l'échelle de compréhension de la rectification égale à 5,77 (cf. Annexe n°15), qui est supérieure à 4, on peut conclure que la rectification est comprise des répondants.

- **H2c :** Appréciation de la mise à jour des données personnelles (Test T pour la comparaison de moyenne d'un échantillon)

La p-value de 0,000/2 = 0 (cf. Annexe n°16), nous permet de rejeter l'hypothèse nulle d'infériorité de la moyenne à 4. Avec une moyenne de l'échelle d'appréciation de la rectification égale à 5,28 (cf. Annexe n°16), qui est supérieure à 4, on peut conclure que la rectification est appréciée des répondants.

- **H3a :** Connaissance du droit à l'effacement des données jadis collectées (Test binomial sur une proportion)

Avec une p-value de 0,000/2 = 0 (cf. Annexe n°17), nous ne rejetons pas l'hypothèse nulle d'infériorité des proportions à 50%. Avec une proportion observée de 24% (cf. Annexe n°17) des répondants connaissant le droit à l'effacement, on peut conclure que le droit à l'effacement n'est pas connu des répondants.

- **H3b :** Compréhension du droit à l'effacement (Test T pour la comparaison de moyenne d'un échantillon)

La p-value de 0,000/2 = 0 (cf. Annexe n°18), nous permet de rejeter l'hypothèse nulle d'infériorité de la moyenne à 4. Avec une moyenne de l'échelle de compréhension de l'effacement égale à 6,29 (cf. Annexe n°18), qui est supérieure à 4, on peut conclure que l'effacement est compris des répondants.

- **H3c :** Appréciation de l'effacement des données jadis collectées (Test T pour la comparaison de moyenne d'un échantillon)

La p-value de 0,000/2 = 0 (cf. Annexe n°19), nous permet de rejeter l'hypothèse nulle d'infériorité de la moyenne à 4. Avec une moyenne de l'échelle d'appréciation de l'effacement égale à 6,52 (cf. Annexe n°19), qui est supérieure à 4, on peut conclure que l'effacement est apprécié des répondants.

- **H4a :** Connaissance de l'existence du label RGPD (Test binomial sur une proportion)

La p-value de 0,000/2 = 0 (cf. Annexe n°20), nous permet de rejeter l'hypothèse nulle de supériorité des proportions à 50%. Avec une proportion observée de 26% (cf. Annexe n°20) des répondants connaissant l'existence du label RGPD, on peut conclure que l'existence du label RGPD n'est pas connue des répondants.

- **H4b :** Compréhension de la signification du label RGPD (Test T pour la comparaison de moyenne d'un échantillon)

La p-value de 0,000/2 = 0 (cf. Annexe n°21), nous permet de rejeter l'hypothèse nulle d'infériorité de la moyenne à 4. Avec une moyenne de l'échelle de compréhension de la signification du label RGPD égale à 4,98 (cf. Annexe n°21), qui est supérieure à 4, on peut conclure que la signification du label RGPD est comprise des répondants.

- **H4c :** Augmentation de la propension à partager les informations personnelles stimulée par le label (Test T pour la comparaison de moyenne d'un échantillon)

La p-value de 0,890/2 = 0,445 (cf. Annexe n°22), ne nous permet pas de rejeter l'hypothèse nulle de supériorité de la moyenne à 4. Avec une moyenne de l'échelle de l'augmentation de la propension à partager les informations personnelles égale à 4,02 (cf. Annexe n°22), qui n'est pas significativement différente de 4, on ne peut pas conclure que la présence du label renforce d'emblée la disposition à partager les informations personnelles.

- **H4d :** Relation entre réticence et partage de données en présence du label (Test d'indépendance du Chi-carré)

Pour vérifier cette hypothèse, nous avons dichotomisé l'échelle d'augmentation de la propension à partager les informations personnelles en présence du logo en attribuant la valeur 0 aux scores allant de 1 à 3 et la valeur 1 aux scores allant de 4 à 7. Nous obtenons alors un tableau de contingence. Nous constatons que 62% des réticents partagent leurs données en présence du label contre 58% des non réticents. (cf. Annexe n°23)

Au test du Chi-carré, la p-value de 0,701 (cf. Annexe n°24), ne nous permet pas de rejeter l'hypothèse nulle d'indépendance entre la réticence et le partage des données. À l'œil nu déjà, l'analyse des données ne nous permet pas de conclure que la présence du label renforce la disposition de partage des données personnelles des réticents par rapport aux non réticents.

- **H5a :** Connaissance du pouvoir d'accès aux données (Test binomial sur une proportion)

La p-value de 0,000/2 = 0 (cf. Annexe n°25), nous permet de rejeter l'hypothèse nulle d'infériorité des proportions à 50%. Avec une proportion observée de 67% (cf. Annexe n°25) des répondants connaissant le droit d'accès, on peut conclure que le droit d'accès est connu des répondants.

- **H5b :** Compréhension du droit d'accès (Test T pour la comparaison de moyenne d'un échantillon)

La p-value de 0,000/2 = 0 (cf. Annexe n°26), nous permet de rejeter l'hypothèse nulle d'infériorité de la moyenne à 4. Avec une moyenne de l'échelle de compréhension de l'accès égale à 5,33 (cf. Annexe n°26), qui est supérieure à 4, on peut conclure que l'accès est compris des répondants.

- **H5c :** Appréciation de l'accès aux données (Test T pour la comparaison de moyenne d'un échantillon)

La p-value de 0,000/2 = 0 (cf. Annexe n°27), nous permet de rejeter l'hypothèse nulle d'infériorité de la moyenne à 4. Avec une moyenne de l'échelle d'appréciation de l'accès égale à 6,33 (cf. Annexe n°27), qui est supérieure à 4, on peut conclure que l'accès est apprécié des répondants.

- **H6a :** Connaissance des activités de cross-selling (Test binomial sur une proportion)

La p-value de 0,000/2 = 0 (cf. Annexe n°28), nous permet de rejeter l'hypothèse nulle d'infériorité des proportions à 50%. Avec une proportion observée de 68% (cf. Annexe n°28) des répondants connaissant les activités de cross-selling, on peut conclure que les activités de cross-selling sont connues des répondants.

- **H6b :** Compréhension du droit d'opposition en cas de cross-selling (Test T pour la comparaison de moyenne d'un échantillon)

La p-value de 0,000/2 = 0 (cf. Annexe n°29), nous permet de rejeter l'hypothèse nulle d'infériorité de la moyenne à 4. Avec une moyenne de l'échelle de compréhension du droit de s'opposer au traitement de données personnelles égale à 5,67 (cf. Annexe n°29), qui est supérieure à 4, on peut conclure que le droit d'opposition est compris des répondants.

- **H6c :** Appréciation de l'opposition en cas de cross-selling (Test T pour la comparaison de moyenne d'un échantillon)

La p-value de 0,000/2 = 0 (cf. Annexe n°30), nous permet de rejeter l'hypothèse nulle d'infériorité de la moyenne à 4. Avec la moyenne de l'échelle d'appréciation de l'opposition égale à 6,56 (cf. Annexe n°30), qui est supérieure à 4, on peut conclure que l'opposition est appréciée des répondants.

- **H7a :** Connaissance de la demande de conservation des preuves de harcèlement (Test binomial sur une proportion)

La p-value de 0,000/2 = 0 (cf. Annexe n°31), nous permet de rejeter l'hypothèse nulle de supériorité des proportions à 50%. Avec une proportion observée de 20% (cf. Annexe n°31) des répondants connaissant le droit de limitation, on peut conclure que le droit de limitation n'est pas connu des répondants.

- **H7b :** Compréhension du droit de limitation (Test T pour la comparaison de moyenne d'un échantillon)

La p-value de 0,000/2 = 0 (cf. Annexe n°32), nous permet de rejeter l'hypothèse nulle d'infériorité de la moyenne à 4. Avec une moyenne de l'échelle de compréhension de la limitation égale à 6,10 (cf. Annexe n°32), qui est supérieure à 4, on peut conclure que la limitation est comprise des répondants.

- **H7c :** Appréciation de la demande de conservation des preuves de harcèlement (Test T pour la comparaison de moyenne d'un échantillon)

La p-value de 0,000/2 = 0 (cf. Annexe n°33), nous permet de rejeter l'hypothèse nulle d'infériorité de la moyenne à 4. Avec une moyenne de l'échelle d'appréciation de la limitation égale à 6,33 (cf. Annexe n°33), qui est supérieure à 4, on peut conclure que la limitation est appréciée des répondants.

B. Connaissance des outils juridiques selon les caractéristiques des répondants (Test d'indépendance de chi-carré)

- **Âge, Sexe, Addiction au smartphone**

Pour chaque variable, nous avons vérifié la condition de réalisation du test d'indépendance de Chi-carré qui est respectée. Tous les effectifs théoriques sont supérieurs à 5.

Figure 12 : Test de Chi-carré entre l'âge, le sexe et l'addiction au smartphone

Eléments	Age	Sexe	Addiction
	p-value		
Portabilité	,964	,084	,805
Rectification	,312	,826	,187
Effacement	,674	,189	,931
Existencelogo	,597	,056	,316
Accès	,182	,485	,761
Crossselling	,472	,784	,284
Limitation	,660	,257	,181

Pour réaliser cette analyse, nous avons regroupé l'âge en deux modalités : 10 à 30 ans puis 31 ans et +. En observant la figure 12, les p-values sont supérieures à 0,05, on ne rejette donc pas l'hypothèse nulle d'indépendance entre la classe d'âge, le sexe, l'addiction et la connaissance des différents éléments juridiques. On en déduit que les caractéristiques des répondants n'influencent pas la connaissance des outils juridiques.

- **Niveau d'éducation**

50% des effectifs théoriques sont inférieurs à 5 (4 répondants non diplômés; 4 répondants issus du primaire-secondaire), la condition d'application du test de chi-carré n'est pas respectée.

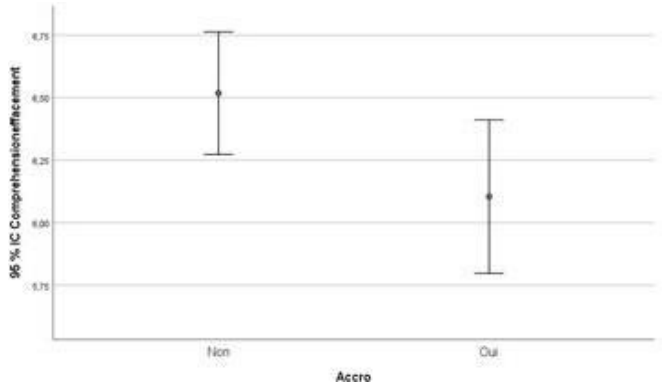
C. Compréhension des outils juridiques selon les caractéristiques des répondants

- **Addiction au smartphone** (Test T pour la comparaison de moyenne de deux échantillons indépendants)

Compréhension effacement par groupe d'addiction

Avec une p-value=0,065, l'hypothèse d'égalité des variances est respectée. Avec une p-value=0,043 (cf. Annexe n°34), on rejette l'hypothèse nulle d'égalité des moyennes entre les deux groupes. Les répondants qui ne se considèrent pas accros semblent mieux comprendre l'effacement (score moyen=6,52) que ceux qui le sont (score moyen=6,10) (cf. Annexe n°34).

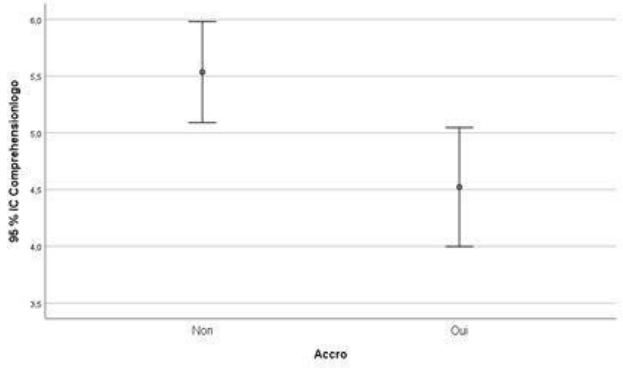
Figure 13 : Distribution de la compréhension de l'effacement selon l'addiction au smartphone



Compréhension label par groupe d'addiction

Avec une p-value=0,009, l'hypothèse d'égalité des variances n'est pas respectée. En considérant la p-value associée égale à 0,004 (cf. Annexe n°35), on rejette l'hypothèse nulle d'égalité des moyennes entre les deux groupes. Les répondants qui ne se considèrent pas accros semblent mieux comprendre le logo (score moyen=5,54) que ceux qui le sont (score moyen=4,52) (cf. Annexe n°35).

Figure 14 : Distribution de la compréhension du label selon l'addiction au smartphone



Compréhension non significative par groupe d'addiction

En dehors de la compréhension de l'effacement et du label, avec des p-values supérieures à 0,05 (cf. Annexe n°36), on ne rejette pas l'hypothèse nulle d'égalité des moyennes. La compréhension des autres outils juridiques ne diffère pas selon l'addiction.

- **Âge** (Test T pour la comparaison de moyennes de deux échantillons indépendants)

Avec des p-values supérieures à 0,05 (cf. Annexe n°37), on ne rejette pas l'hypothèse nulle d'égalité des moyennes. La compréhension des outils juridiques ne diffère pas selon les classes d'âge.

- **Sexe** (Test T pour la comparaison de moyenne de deux échantillons indépendants)

Avec des p-values supérieures à 0,05 (cf. Annexe n°38), on ne rejette pas l'hypothèse nulle d'égalité des moyennes. La compréhension des outils juridiques ne diffère pas selon le sexe.

- **Niveau d'éducation** (Anova parce que nous avons plus de deux groupes)

L'hypothèse d'homogénéité des variances a été vérifiée grâce au test de Levene et est respectée (cf. Annexe n°39). Pour la compréhension de la rectification et de l'opposition, l'hypothèse d'homogénéité des variances n'étant pas respectée, nous effectuons le test de Welch (cf. Annexe n°40). Avec des p-values supérieures à 0,05 (cf. Annexe n°39 et 40), on ne rejette pas l'hypothèse nulle d'égalité des moyennes. La compréhension des outils juridiques ne diffère pas selon le niveau d'étude.

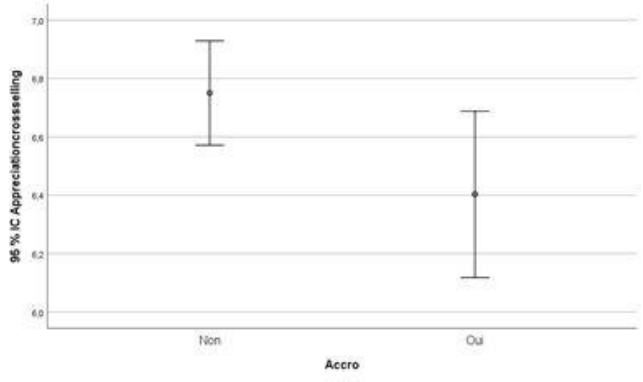
D. Appréciation des outils juridiques selon les caractéristiques des répondants

- **Addiction au smartphone** (Test T pour la comparaison de moyenne de deux échantillons indépendants)

Appréciation de l'opposition selon l'addiction

L'hypothèse d'égalité des variances n'étant pas respectée, on considère la p-value associée. Avec une p-value de 0,042(< 5%) (cf. Annexe n°41), on rejette l'hypothèse nulle d'égalité des moyennes. L'appréciation de l'opposition diffère selon qu'on se considère accro ou pas. Les non-accros semblent plus apprécier l'opposition (score moyen=6,75) que ceux qui se considèrent accros (score moyen=6,40) (cf. Annexe n°41).

Figure 15 : Distribution de l'appréciation de l'opposition selon l'addiction au smartphone



Appréciation non significative selon l'addiction au smartphone

Les p-values au test de Levene sont supérieures à 0,05 (cf. Annexe n°42), l'hypothèse d'égalité des variances est respectée (sauf pour l'appréciation de l'accès où nous considérons plutôt la p-value correspondante à l'hypothèse de variances inégales). En dehors de l'appréciation de l'opposition, avec des p-values supérieures à 0,05 (cf. Annexe n°42), on ne rejette pas l'hypothèse nulle d'égalité des moyennes. L'appréciation des autres outils juridiques ne diffère pas selon l'addiction.

- **Âge** (Test T pour la comparaison de moyenne de deux échantillons indépendants)

Renforcement label selon l'âge

L'hypothèse d'homogénéité des variances est respectée. Avec une p-value de 0,006 (< 5%) (cf. Annexe n°43), on rejette l'hypothèse nulle d'égalité des moyennes. Le renforcement dû à la présence du label diffère selon la classe d'âge. La présence du logo renforce la disposition des moins âgés à partager leurs informations (score moyen=4,43) alors qu'elle ne met pas en confiance les répondants qui sont âgés de plus de 30 ans (score moyen=3,45) (cf. Annexe n°43).

Appréciation non significative selon l'âge

Les p-values au test de Levene sont supérieures à 0,05 (cf. Annexe n°44), l'hypothèse d'égalité des variances est respectée (sauf pour l'appréciation de l'accès et de l'opposition où nous considérons plutôt la p-value correspondante à l'hypothèse de variances inégales).
Avec des p-values supérieures à 0,05 (cf. Annexe n°44), on ne rejette pas l'hypothèse nulle d'égalité des moyennes. L'appréciation des outils juridiques autres que le label ne diffère pas selon la classe d'âge.

- **Sexe** (Test T pour la comparaison de moyenne de deux échantillons indépendants)

Les p-values au test de Levene sont supérieures à 0,05 (cf. Annexe n°45), l'hypothèse d'égalité des variances est respectée (sauf pour l'appréciation de la portabilité et celle de l'effacement où nous considérons plutôt la p-value correspondante à l'hypothèse de variances inégales). Avec des p-values supérieures à 0,05 (cf. Annexe n°45), on ne rejette pas l'hypothèse nulle d'égalité des moyennes. L'appréciation des outils juridiques ne diffère pas selon le sexe.

- **Niveau d'éducation (**Anova parce que nous avons plus de deux groupes**)**

Appréciation rectification selon le niveau d'éducation

L'hypothèse d'homogénéité des variances est respectée. Avec une p-value de 0,006 (< 5%) (cf. Annexe n°46), on rejette l'hypothèse nulle d'égalité des moyennes.
L'appréciation de la rectification diffère selon le niveau d'éducation.

À l'aide du test de comparaisons multiples de Bonferroni, on constate une différence significative entre l'appréciation de la rectification des répondants ayant un niveau primaire-secondaire d'une part et ceux ayant un niveau bachelier et master-doctorat d'autre part. Les répondants ayant un niveau primaire-secondaire n'apprécient pas la rectification (score moyen=2,75) contrairement à ceux qui ont un niveau d'instruction plus élevé (bachelier et master-doctorat : score moyen=5,41) (cf. Annexe n°46).

Appréciation non significative selon le niveau d'éducation

L'hypothèse d'homogénéité des variances a été vérifiée grâce au test de Levene et est respectée (cf. Annexe n°47). Pour l'appréciation de l'effacement et de l'accès, l'hypothèse d'homogénéité des variances n'étant pas respectée, nous effectuons le test de Welch (cf. Annexe n°48). Le test robuste n'a pu être effectué pour l'appréciation de l'effacement, car au moins un groupe possède une variance de 0 (cf. Annexe n°48). Avec des p-values supérieures à 0,05 (cf. Annexe n°47 et 48), on ne rejette pas l'hypothèse nulle d'égalité des moyennes. L'appréciation de ces outils juridiques ne diffère pas selon le niveau d'étude.

VI. Récapitulatif des résultats

En guise de synthèse des résultats, l'introduction d'un tableau récapitulatif permet une vision d'ensemble des statuts de vérification des hypothèses préalablement posées. Ainsi, le tableau ci-dessous est structuré comme suit : la première colonne rappelle l'hypothèse testée. La seconde indique l'outil statistique employé. La troisième colonne montre si l'hypothèse a été vérifiée ou non. La quatrième colonne souligne le sens observé par comparaison avec l'hypothèse initiale. Enfin, la dernière colonne propose une formulation du résultat obtenu.

	Outil Stat.	**Statut de l'hypothèse**	**Sens**	**Résultat**
H1a: proportion de connaissance de la portabilité > 50%	Binomial	Non vérifiée		Il n'est pas vérifié que > 50% des répondants connaissent le droit à la portabilité.
H1b: compréhension de portabilité > 4 sur une échelle de 7	Test T	Vérifiée	Attendu	Il est vérifié que la compréhension de la portabilité > 4 sur une échelle de 7. Bien que la valeur de 4,62 est proche du seuil neutre de compréhension. De fait, avec une telle moyenne, le droit à la portabilité s'avère être le droit le moins compris des répondants.
H1c: appréciation de portabilité > 4 sur une échelle de 7	Test T	Vérifiée	Inverse	Il est vérifié que l'appréciation de la portabilité < 4 sur une échelle de 7. En l'occurrence, avec une moyenne de 3,38, le droit à la portabilité est le moins apprécié des répondants.
H2a: proportion de connaissance de la mise à jour des données > 50%	Binomial	Vérifiée	Attendu	Il est vérifié que > 50% des répondants connaissent la possibilité de mettre à jour leurs données personnelles.
H2b: compréhension de rectification > 4 sur une échelle de 7	Test T	Vérifiée	Attendu	Il est vérifié que la compréhension de la rectification > 4 sur une échelle de 7.
H2c: appréciation mise à jour > 4 sur une échelle de 7	Test T	Vérifiée	Attendu	Il est vérifié que l'appréciation de pouvoir mettre à jour ses données personnelles > 4 sur une échelle de 7.
H3a: proportion de connaissance de l'effacement des données jadis collectées > 50%	Binomial	Vérifiée	Inverse	Il est vérifié que < 50% des répondants connaissent la possibilité d'effacer des données jadis collectées.

H3b: compréhension de l'effacement > 4 sur une échelle de 7	Test T	Vérifiée	Attendu	Il est vérifié que la compréhension de l'effacement > 4 sur une échelle de 7.
H3c: appréciation effacer données jadis collectées > 4 sur une échelle de 7	Test T	Vérifiée	Attendu	Il est vérifié que l'appréciation d'effacer des données jadis collectées > 4 sur une échelle de 7. Avec une moyenne de 6,52, le droit d'effacer des données jadis collectées est le second droit le plus apprécié des répondants.
H4a: proportion de connaissance du label RGPD > 50%	Binomial	Vérifiée	Inverse	Il est vérifié que < 50% des répondants connaissent l'existence du label RGPD.
H4b: compréhension signification label > 4 sur une échelle de 7	Test T	Vérifiée	Attendu	Il est vérifié que la compréhension de la signification du label RGPD > 4 sur une échelle de 7.
H4c: propension à partager en présence du label > 4 sur une échelle de 7	Test T	Non vérifiée		Il n'est pas vérifié que la propension à partager les données personnelles en présence du label > 4 sur une échelle de 7.
H4d: En présence du label, les réticents partagent + que les non réticents	Chi-carré	Non vérifiée		Il n'est pas vérifié que la présence du label renforce la disposition de partage des données personnelles des réticents par rapport aux non réticents. Cependant, l'observation souligne une tendance non significative des réticents (62% d'entre eux) à davantage partager leurs données en présence du label en comparaison avec les non réticents (58% d'entre eux).
H5a: proportion connaissance accès aux données > 50%	Binomial	Vérifiée	Attendu	Il est vérifié que > 50% des répondants connaissent la possibilité d'accéder aux données personnelles détenues par un organisme.
H5b: compréhension accès > 4 sur une échelle de 7	Test T	Vérifiée	Attendu	Il est vérifié que la compréhension du droit de demander l'accès à ses données personnelles > 4 sur une échelle de 7.
H5c: appréciation accès > 4 sur une échelle de 7	Test T	Vérifiée	Attendu	Il est vérifié que l'appréciation de la possibilité d'accéder à ses données personnelles > 4 sur une échelle de 7.
H6a: Proportion connaissance cross-selling > 50%	Binomial	Vérifiée	Attendu	Il est vérifié que > 50% des répondants connaissent l'existence des activités de cross-selling.
H6b: compréhension opposition > 4 sur une échelle de 7	Test T	Vérifiée	Attendu	Il est vérifié que la compréhension du droit d'opposition en cas de cross-selling > 4 sur une échelle de 7.

H6c: appréciation opposition cross-selling > 4 sur une échelle de 7	Test T	Vérifiée	Attendu	Il est vérifié que l'appréciation du pouvoir de s'opposer au traitement des données personnelles en cas de cross-selling > 4 sur une échelle de 7. En l'occurrence, le droit d'opposition en cas de cross-selling est, avec une moyenne de 6,56, le droit le plus apprécié des répondants.
H7a: proportion connaissance conservation preuves de harcèlement > 50%	Binomial	Vérifiée	Inverse	Il est vérifié que < 50% des répondants connaissent la possibilité de demander la conservation des preuves de harcèlement auprès d'un organisme.
H7b: compréhension limitation > 4 sur une échelle de 7	Test T	Vérifiée	Attendu	Il est vérifié que la compréhension du droit de limitation (demander le gel temporaire de l'utilisation des données) > 4 sur une échelle de 7.
H7c: appréciation conservation preuves harcèlement > 4 sur une échelle de 7	Test T	Vérifiée	Attendu	Il est vérifié que l'appréciation du pouvoir de demander la conservation des preuves de harcèlement auprès d'un organisme > 4 sur une échelle de 7.
Hxa': caractéristiques des répondants influent sur la connaissance des outils juridiques	Chi-carré	Non vérifiée		Il n'est pas vérifié que les caractéristiques des répondants influencent la connaissance des outils juridiques.
Hxb': caractéristiques des répondants influent sur la compréhension des outils juridiques	Test T, Anova	Partiellement vérifiée		Il n'est pas vérifié que les caractéristiques des répondants influencent la compréhension des outils juridiques sauf pour les non-accros qui semblent mieux comprendre l'effacement et la signification du label
Hxc': caractéristiques des répondants influent sur l'appréciation des outils juridiques	Test T, Anova	Partiellement vérifiée		Il n'est pas vérifié que les caractéristiques des répondants influencent l'appréciation des outils juridiques sauf pour les non-accros qui semblent mieux apprécier l'opposition ; pour les moins âgés qui partagent plus leurs données en présence du label en comparaison avec leurs aînés davantage méfiants; pour les moins instruits (primaire-secondaire) qui n'apprécient pas la rectification contrairement à ceux qui ont un niveau d'instruction plus élevé (bachelier et master-doctorat)

Partie 3 : Conclusions

I. Conclusion de l'étude

Notre recherche avait pour objectif de répondre à la question centrale suivante : "*Quel est l'impact du RGPD sur la confiance des consommateurs ?*". Afin d'assurer une profondeur de réponse à la problématique de départ, nous avons préalablement défini un fil conducteur composé de 4 sous-questions distinctes, chacune apportant son lot de réponses au sujet de recherche.

Tout d'abord, la première sous-question visait à identifier les principes du RGPD qui causent la confiance chez les consommateurs, traduits ici par un niveau de réponse plus élevé sur l'échelle d'appréciation des outils juridiques. En l'occurrence, nous pouvons apporter à la littérature existante que le droit à l'opposition en cas de cross-selling (moyenne = 6,56) et à l'effacement des données jadis collectées (moyenne = 6,52) sont les plus appréciés des consommateurs et que leur conscience d'exercice est gage d'une plus grande sérénité lors de la navigation en ligne. Également, nous sommes en mesure d'avancer un résultat inattendu : le droit à la portabilité des données n'est pas apprécié des consommateurs. Ce résultat contraire à l'hypothèse posée en amont de l'analyse statistique peut s'expliquer de diverses manières. D'une part, le droit à la portabilité est le moins compris de tous les droits (moyenne = 4,62). D'autre part, nous pouvons imaginer que les consommateurs aient déjà intégré les risques de fuites de données au moment de l'extraction puis du transfert vers une plateforme alternative, comme avancé par le Working Party G29 en 2016 (Article 29 Working Party, 2016).

Ensuite, la seconde sous-question cherchait à déterminer le degré d'influence de variables sociodémographiques sur la confiance des consommateurs née des outils du RGPD. À cet égard, nous sommes disposés à compléter la littérature actuelle en matière de labels de

protection de données, en soulignant pour la première fois l'interprétation des consommateurs à la vue d'un label de conformité au RGPD. En effet, selon l'âge nous pouvons souligner un résultat dichotomique : par similarité avec les résultats de Turow en 2001, les internautes les moins âgés (10-30 ans) se sentent rassurés par la présence du label et partagent plus leurs données que leurs aînés (31 ans et +) qui eux, révèlent une véritable méfiance traduite par un partage de données moindre. Nous pouvons ici juger utile de rappeler les propos tenus par Rifon et al. pour tenter d'expliquer semblable observation. De fait, nous pouvons imaginer que l'esprit critique davantage aiguisé des plus âgés oriente la vision du label en tant que "simple illusion de protection de la vie privée" (Rifon & al., 2005). En ce sens, nous pouvons mettre en exergue le fait que les plus âgés ne sont pas réceptifs à la stratégie de co-branding par le label avancée par Miyazaki et Krishnamurthy (Miyazaki et Krishnamurthy, 2002). Par ailleurs, sur base du niveau d'études, nous avons décelé une différence significative dans l'appréciation du droit à la rectification. Effectivement, les moins instruits (primaire-secondaire) n'apprécient pas le droit à la rectification au contraire des niveaux d'instruction plus élevés (bachelier et master-doctorat).

Enfin, les deux dernières sous-questions revêtent une forme créative en évaluant l'influence de variables comportementales, comme l'addiction au smartphone ou la réticence habituelle au partage de données, sur les dimensions de connaissance, de compréhension et d'appréciation des outils du RGPD. Au terme de notre analyse, nous pouvons conclure que les utilisateurs ne s'estimant pas "accros" au smartphone apprécient davantage le recours à l'opposition au traitement de données en comparaison avec les addicts. De plus, les non-accros démontrent une meilleure compréhension du droit à l'effacement ainsi que de la signification du label RGPD. Notre recherche permet donc de souligner que l'addiction au smartphone, sans prise de recul nécessaire, expose les utilisateurs à une plus grande vulnérabilité numérique. En dernier lieu, malgré une tendance non significative des réticents contre les non réticents à davantage partager leurs données en présence du label, nous ne pouvons pas certifier que la réticence habituelle au partage de données soit inhibée par le sceau de conformité.

II. Implications managériales, éthiques et scientifiques

Premièrement, à la lecture des résultats de l'enquête, nous constatons que le droit d'accès est la troisième action protectrice la mieux valorisée (moyenne = 6,33) par nos répondants. Or, la littérature nous révélait que les entreprises n'assurent pas suffisamment la visibilité du droit d'accès étant donné que 39% des interfaces web exigent de l'internaute un minimum de 5 minutes de recherche avant de parvenir aux sections en la matière (L'Hoiry et Norris, 2015). Dès lors, nous pouvons recommander aux gestionnaires et plus particulièrement aux équipes IT de veiller à ce que l'ergonomie des sites web soit davantage optimisée afin de raccourcir le chemin permettant aux consommateurs d'assouvir leur intérêt déclaré envers l'accès aux données personnelles.

Deuxièmement, parmi les découvertes prépondérantes de notre étude figurent le manque d'intérêt et de connaissance des consommateurs envers le droit à la portabilité. Néanmoins, nous voyons ici une opportunité managériale visant à augmenter tant le bien-être des entreprises que celui des consommateurs. En effet, nous recommandons aux gestionnaires de davantage promouvoir et de clarifier la possibilité offerte aux utilisateurs de réutiliser leurs données générées auprès d'une plateforme vers une autre. De cette manière, d'une part les consommateurs n'ont pas à abandonner des données précieuses à chaque changement de service (1) comme par exemple le transfert de goûts musicaux permettant à l'intelligence artificielle de proposer des playlists pertinentes sur la nouvelle plateforme. D'autre part, dans le cas où les consommateurs s'exercent davantage à la portabilité, un avantage concurrentiel est susceptible de se dessiner pour les entreprises. Effectivement, en accédant à des données détenues par d'autres acteurs de l'industrie, les entreprises sont à même de penser de nouveaux modèles d'affaires centrés sur ces données (2). Pour autant que les guidelines du RGPD soient respectées sous peine de se voir infliger une amende allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial (Article 83, RGPD).

Troisièmement, d'un point de vue éthique, alors qu'à l'heure d'écrire ces lignes l'application "FaceApp*"* menace la vie privée des utilisateurs (Faljaoui, 2019), nous pouvons affirmer que nous avons conscientisé les répondants sur la manière de se protéger des vices de l'ère numérique. En témoigne la majorité des réponses à la question ouverte facultative mentionnant un questionnaire "instructif" (cf. Annexe n°49).

Toujours selon un angle éthique, notre étude prend la défense des plus jeunes au regard de leur vulnérabilité en présence d'un label et nous recommandons donc aux autorités de faire preuve de surveillance quant à l'usurpation éventuelle des labels RGPD.

Dernièrement, concernant les apports scientifiques, notre mémoire-recherche aura permis de traiter une thématique récente et d'apporter à la littérature des divergences sociodémographiques et comportementales dans la compréhension et l'appréciation des outils de protection du RGPD. Également, d'un point de vue marketing, notre étude ajoute à la littérature existante les effets des stratégies de co-branding par le label RGPD. À titre d'illustration, nous avons pu découvrir que les citoyens de plus de 30 ans ne sont pas réceptifs au co-branding par le label RGPD au contraire des répondants moins âgés.

III. Limites de l'étude

Toute recherche implique de poser un regard critique sur l'interprétation des résultats obtenus. En effet, à l'issue de notre étude, nous recensons différentes limites dont la conscience requiert au lecteur d'interpréter les découvertes avec précaution.

En premier lieu, malgré le regroupement en deux tranches d'âge, nous observons une sous-représentation des répondants appartenant à la catégorie des 31 ans et + (51 individus contre 72), ce qui a pu par exemple sous-estimer la moyenne de confiance des plus âgés en présence du label RGPD. Par ailleurs, nous remarquons également une sous-représentation des niveaux d'études inférieurs impliquant une probable sous-évaluation du niveau d'appréciation de la rectification sur base de cette modalité. De plus, la taille de l'échantillon (n=123) n'assure pas une représentativité exhaustive, nous ne sommes donc pas en mesure d'inférer les résultats à la population.

Un autre type de limite a trait aux conditions expérimentales des questionnaires diffusés sur internet. De fait, une telle méthode ne permet pas au chercheur d'assurer un contrôle des conditions de réponses et nous ne pouvons être certains que le niveau de concentration des répondants eut été optimal.

En outre, parmi les 61 réponses à la question ouverte facultative, 7 répondants déclarent une mauvaise compréhension de certaines sections du questionnaire (cf. Annexe n°49), ce qui est susceptible de générer des réponses peu en phase avec le réel sentiment de ces répondants.

D'autre part, les avis divergent sur la validité minimale de l'alpha de Cronbach, qui pour rappel, est de 0.54 en ce qui concerne l'échelle d'appréciation. Dès lors, bien que non rejetée selon la "rule of thumb" (cf. Annexe n°50), une faible valeur de l'alpha de Cronbach peut signifier un manque de cohérence dans la mesure de l'appréciation des outils du RGPD et ainsi biaiser les résultats des répondants pour cette dimension.

Enfin, nous jugeons adéquat d'insérer une dernière limite propre au profil d'étudiant. En effet, nous ne sommes encore qu'au début de la courbe d'apprentissage en termes d'administration de questionnaires et nous sommes convaincus qu'avec l'expérience, la qualité du design des questionnaires suivra une courbe ascendante.

IV. Futures recherches

Compte tenu des limites et des recommandations managériales de notre étude, nous sommes aptes à proposer différentes pistes de recherches futures.

En premier lieu, le format d'une enquête quantitative ayant démontré ses limites, il serait judicieux de combiner une telle approche à une méthode de collecte davantage qualitative afin d'une part, contrôler les conditions expérimentales et d'autre part, bénéficier d'une plus grande profondeur d'investigation.

Également, nous estimons que la recherche future apprécierait de profiter d'un temps de diffusion d'enquête prolongé dans l'optique d'élargir l'échantillon et d'ainsi jouir d'une meilleure répartition des répondants selon l'âge ou le niveau d'éducation. Dans pareilles conditions, la généralisation des résultats à plus grande envergure s'en trouverait simplifiée. De plus, un nombre plus important d'individus constituant l'échantillon permettrait de mieux souligner l'intensité d'influence des modalités sociodémographiques et comportementales introduites dans notre modèle de recherche.

Par ailleurs, au vu des 7 répondants à la question ouverte ayant déclaré une mauvaise compréhension partielle du questionnaire (cf. Annexe n°49), nous recommandons aux futurs mémorants d'inclure obligatoirement ce type de question finale afin d'intégrer la présence de nouveaux biais lors de la prise de recul nécessaire aux découvertes.

Enfin, la thématique du RGPD se rapportant au monde "connecté", nous jugeons opportun pour les futurs chercheurs de considérer de nouvelles tendances comportementales émanant de l'ère numérique afin d'en vérifier l'influence sur la confiance stimulée par le RGPD. Dès lors, nous voyons en cette étude la possibilité de servir de rampe de lancement pour d'autres recherches tout aussi intéressantes que prometteuses.

Bibliographie

Akcura, M. T., & Srinivasan, K. (2005). Research note: Customer intimacy and cross-selling strategy. *Management Science*, 51(6), 1007-1012. doi:10.1287/mnsc.1050.0390

Akçura, M. T., Özdemir, Z. D., & Altınkemer, K. (2009). Privacy, customization, and cross-selling of information. *Journal of Organizational Computing and Electronic Commerce*, 19(2), 112-132. doi:10.1080/10919390902821283

André, Q., Carmon, Z., Wertenbroch, K., Crum, A., Frank, D., Goldstein, W., Yang, H. (2018). Consumer choice and autonomy in the age of artificial intelligence and big data. *Customer Needs and Solutions*, 5(1), 28-37. doi:10.1007/s40547-017-0085-8

Anshari, M., Almunawar, M. N., Lim, S. A., & Al-Mudimigh, A. (2018). Customer relationship management and big data enabled: Personalization & customization of services. *Applied Computing and Informatics*, doi:10.1016/j.aci.2018.05.004

Article 29 Working Party. (2016). *Guidelines on the right to data portability*. En ligne sur https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf (Document pdf consulté le 28/04/19)

Astié, P., Breillat, D. & Lageot, C. (2017). Repères étrangers: (1er avril – 30 juin 2017). *Pouvoirs*, 163(4), 141-158. doi:10.3917/pouv.163.0141.

Auschaitrakul, S., & Mukherjee, A. (2017). Online display advertising: The influence of web site type on advertising effectiveness: online display advertising. *Psychology & Marketing*, 34(4), 463-480. doi:10.1002/mar.21000

Baksi, S., Bose, P., & Xiang, D. (2017). Credence goods, misleading labels, and quality differentiation. *Environmental and Resource Economics*, 68(2), 377-396. doi:10.1007/s10640-016-0024-4

Bartoli, E. (2009). Children's data protection vs marketing companies. *International Review of Law, Computers & Technology*, 23(1-2), 35-45. doi:10.1080/13600860902742612

Bastin, G., & Tubaro, P. (2018). Le moment big data des sciences sociales. *Revue Française De Sociologie*, 59(3), 375-394. doi:10.3917/rfs.593.0375

Bergel, M., & Brock, C. (2018). The impact of switching costs on customer complaint behavior and service recovery evaluation. *Journal of Service Theory and Practice*, 28(4), 458-483. doi:10.1108/JSTP-02-2017-0035

Bergin, T. (2018). *How a data mining giant got me wrong*. Reuters. En ligne sur https://www.reuters.com/article/us-data-privacy-acxiom-insight/how-a-data-mining-giant-got-me-wrong-idUSKBN1H513K (Consulté le 25/05/19)

Berkelaar, B. L., & Buzzanell, P. M. (2015). Online employment screening and digital career capital: Exploring employers' use of online information for personnel selection. *Management Communication Quarterly*, 29(1), 84-113. doi:10.1177/0893318914554657

Bertholet, C. & Létourneau, L. (2017). Ubériser l'État ?. *Le journal de l'école de Paris du management*, 128(6), 37-44. doi:10.3917/jepam.128.0037.

Bleier, A., & Eisenbeiss, M. (2015). The importance of trust for personalized online advertising. *Journal of Retailing*, 91(3), 390-409. doi:10.1016/j.jretai.2015.04.001

Bonroy, O., & Constantatos, C. (2008). On the use of labels in credence goods markets. *Journal of Regulatory Economics*, 33(3), 237-252. doi:10.1007/s11149-008-9058-z

Boyadjian, J. (2018). Menger (Pierre-Michel), Paye (Simon), dir., Big data et traçabilité numérique. Les sciences sociales face à la quantification massive des individus, Paris, Collège de France, 2017, 218 p.. *Politix*, 122(2), 234-237. doi:10.3917/pox.122.0234.

Brown, M. L., & Kros, J. F. (2003). Data mining and the impact of missing data. *Industrial Management & Data Systems*, 103(8), 611-621. doi:10.1108/02635570310497657

Bucklin, R. E., Lehmann, D. R., & John D. C. Little. (1998). From decision support to decision automation: A 2020 vision. *Marketing Letters*, 9(3), 235-246. doi:10.1023/A:1008047504898

Burnham, T. A., Frels, J. K., & Mahajan, V. (2003). Consumer switching costs: A typology, antecedents, and consequences. *Journal of the Academy of Marketing Science*, 31(2), 109-126. doi:10.1177/0092070302250897

Bylander, J. (2014). predictive analytics: The power to predict who will click, buy, lie, or die. *Health Affairs*, 33(7), 1302.

Camacho, S., Hassanein, K., & Head, M. (2014). Understanding the factors that influence the perceived severity of cyber-bullying. Paper presented at the , *8527* 133-144. doi:10.1007/978-3-319-07293-7_13

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Raghav Rao, H. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems*, 83, 47-56. doi:10.1016/j.dss.2015.12.007

Chiranjeevi, H. S., Shenoy, M. K., & Sundar, D. S. (2018). Integrating on-premises data with customer relationship management application on cloud: A hybrid IT infrastructure support service. *Cogent Engineering*, 5(1) doi:10.1080/23311916.2018.1462755

Chirica, S. (2017). the main novelties and implications of the new general data protection regulation. *"Perspectives of Business Law" Journal*, 6(1), 159-176.

Cliza, M., & Spataru-Negura, L. (2018). The general data protection regulation: What does the public authorities and bodies need to know and to do? the rise of the data protection officer. *Juridical Tribune Journal = Tribuna Juridica*, 8(2), 489-501.

CNIL. (2018). *Le droit à la limitation du traitement : geler l'utilisation de vos données*. Commission nationale de l'informatique et des libertés. En ligne sur https://www.cnil.fr/fr/le-droit-la-limitation-du-traitement-geler-lutilisation-de-vos-donnees (Consulté le 27/05/19)

Computer Fraud & Security. (2017). Uber confesses to covering up breach. doi:10.1016/S1361-3723(17)30102-1

Courtheoux, R. J. (2003). Marketing data analysis and data quality management. *Journal of Targeting, Measurement and Analysis for Marketing*, *11*(4), 299.

Crain, M. (2018). The limits of transparency: Data brokers and commodification. *New Media & Society*, 20(1), 88-104. doi:10.1177/1461444816657096

Curtis, S. R., Carre, J. R., & Jones, D. N. (2018). Consumer security behaviors and trust following a data breach. *Managerial Auditing Journal*, 33(4), 425-435. doi:10.1108/MAJ-11-2017-1692

Doorn, J. v., & Hoekstra, J. C. (2013). Customization of online advertising: The role of intrusiveness. *Marketing Letters*, 24(4), 339-351. doi:10.1007/s11002-012-9222-1

Dujardin, C. (2019). *Niveau de diplôme de la population de 25 ans et plus*. Iweps. En ligne sur https://www.iweps.be/indicateur-statistique/niveau-de-diplome-de-population-de-25-ans-plus/ (Consulté le 12/07/19)

Engels, B. (2016). Data portability among online platforms. *Internet Policy Review*, 5(Issue 2) doi:10.14763/2016.2.408

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

European Data Protection Supervisor. (2015). *Relever les défis des données massives*. En ligne sur https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_fr.pdf (Document pdf consulté le 25/04/19)

Even, A., Shankaranarayanan, G., & Berger, P. D. (2010). Inequality in the utility of customer data: Implications for data management and usage. *Journal of Database Marketing & Customer Strategy Management*, 17(1), 19-35. doi:10.1057/dbm.2010.1

Faljaoui, A. (2019). *La face cachée de FaceAPP*. RTBF. En ligne sur https://www.rtbf.be/classic21/article/detail_la-face-cachee-de-faceapp?id=10276377 (Consulté le 20/07/2019)

Feiereisen, S., Rasolofoarison, D., De Valck, K., & Schmitt, J. (2019). Understanding emerging adults' consumption of TV series in the digital age: A practice-theory-based approach. *Journal of Business Research*, 95, 253-265. doi:10.1016/j.jbusres.2018.08.024

Ferguson, J. L. (2014). Implementing price increases in turbulent economies: Pricing approaches for reducing perceptions of price unfairness. *Journal of Business Research*, 67(1), 2732-2737. doi:10.1016/j.jbusres.2013.03.023

Forbes. (2019). *The World's Most Valuable Brands*. En ligne sur https://www.forbes.com/powerful-brands/list/#tab:rank (Consulté le 25/07/19)

García-Gil, D., Luengo, J., García, S., & Herrera, F. (2019). Enabling smart data: Noise filtering in big data classification. *Information Sciences*, 479, 135-152. doi:10.1016/j.ins.2018.12.002

Gombeski, W. R., Kantor, D., Bendycki, N. A., & Wack, J. (2002). Improve your marketing effectiveness and net income through better prospecting. *Health Marketing Quarterly*, 19(4), 3-19. doi:10.1300/J026v19n04_02

Gozlan, A. (2018). Eléments pour une psychopathologie du virtuel : Le harcèlement virtuel/Elements concerning psychopathology in the virtual sphere: Cyberbullying. *L'Evolution Psychiatrique*, 83(3), 457. doi:10.1016/j.evopsy.2018.03.003

Graef, I. (2015). Mandating portability and interoperability in online social networks: Regulatory and competition law issues in the european union. *Telecommunications Policy*, 39(6), 502-514. doi:10.1016/j.telpol.2015.04.001

Grow, D. (2017). *Surefire ways to annoy a customer with bad data*. Business. En ligne sur https://www.business.com/articles/surefire-ways-to-annoy-a-customer-with-bad-data/ (Consulté le 10/06/19)

Guo, F., & Qin, H. (2017). Data mining techniques for customer relationship management. *Journal of Physics: Conference Series*, 910, 12021. doi:10.1088/1742-6596/910/1/012021

Hartemo, M. (2016). Email marketing in the era of the empowered consumer. *Journal of Research in Interactive Marketing*, 10(3), 212-230. doi:10.1108/JRIM-06-2015-0040

Haug, A., Zachariassen, F., & Liempd, D. (2011). The costs of poor data quality. *Journal of Industrial Engineering and Management*, 4(2), 168-193. doi:10.3926/jiem.v4n2.p168-193

Hazen, B. T., Boone, C. A., Ezell, J. D., & Jones-Farmer, L. A. (2014). Data quality for data science, predictive analytics, and big data in supply chain management: An introduction to the problem and suggestions for research and applications. *International Journal of Production Economics*, 154, 72-80. doi:10.1016/j.ijpe.2014.04.018

Heimbach, I., Kostyra, D. S., & Hinz, O. (2015). Marketing automation. *Business & Information Systems Engineering*, 57(2), 129-133. doi:10.1007/s12599-015-0370-8

Herrando, C., Jimenez-Martinez, J., & Martin-De Hoyos, M. J. (2019). Tell me your age and I tell you what you trust: The moderating effect of generations. *Internet Research*, doi:10.1108/IntR-03-2017-0135

Hicken, M. (2013). *Find out what Big Data knows about you (it may be very wrong)*. CNN Money. En ligne sur https://money.cnn.com/2013/09/05/pf/acxiom-consumer-data/ (Consulté le 26/06/19)

Hinz, O., Hann, I., & Spann, M. (2011). Price discrimination in E-commerce? an examination of dynamic pricing in name-your-own price markets. *MIS Quarterly*, 35(1), 81-98. doi:10.2307/23043490

Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult facebook users. *Journal of Interactive Advertising*, 10(2), 28-45. doi:10.1080/15252019.2010.10722168

Jai, T. (., & King, N. J. (2016). Privacy versus reward: Do loyalty programs increase consumers' willingness to share personal information with third-party advertisers and data brokers? *Journal of Retailing and Consumer Services*, 28, 296-303. doi:10.1016/j.jretconser.2015.01.005

Jocard, A. (2018). *Données personnelles : plaintes collectives contre les GAFAM à Paris*. RTL Info. En ligne sur https://www.rtl.be/info/magazine/hi-tech/donnees-personnelles-plaintes-collectives-contre-les-gafam-a-paris--1026004.aspx (Consulté le 22/12/18)

Jones, M. A., Mothersbaugh, D. L., & Beatty, S. E. (2002). Why customers stay: Measuring the underlying dimensions of services switching costs and managing their differential strategic outcomes. *Journal of Business Research, 55*(6), 441-450. doi:10.1016/S0148-2963(00)00168-5

Kamleitner, B., & Mitchell, V. W. (2018). Can consumers experience ownership for their personal data? From issues of scope and invisibility to agents handling our digital blueprints. In J. Peck & S. Shu (Eds.), *Psychological ownership and consumer behavior* (pp. 91–118).

Katz M. et Shapiro C. (1994). Systems competition and network effects, *Journal of Economic Perspectives*, 8, 2, 93-115

Korinman, M. (2017). The Art of the deal. *Outre-Terre*, 50(1), 9-28. doi:10.3917/oute1.050.0009.

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, 140(4), 1073-1137. doi:10.1037/a0035618

Krämer, J., & Stüdlein, N. (2019). Data portability, data disclosure and data-induced switching costs: Some unintended consequences of the general data protection regulation. *Economics Letters*, 181, 99-103. doi:10.1016/j.econlet.2019.05.015

Labrecque, L. I., Markos, E., & Milne, G. R. (2011). Online personal branding: Processes, challenges, and implications. *Journal of Interactive Marketing*, 25(1), 37-50. doi:10.1016/j.intmar.2010.09.002

Lambin, J.J., de Moerloose, Ch. (2016). *Marketing Stratégique et Opérationnel*. 9° Edition. Paris, Dunod. pp. 191-195

Lambrecht, M. (2016). L'économie des plateformes collaboratives. *Courrier hebdomadaire du CRISP*, 2311-2312(26), 5-80. doi:10.3917/cris.2311.0005.

Larose, R., & Rifon, N. J. (2007). Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *The Journal of Consumer Affairs, 41*(1), 127-149. doi:10.1111/j.1745-6606.2006.00071.x

Lefèvre, N., & Taverne, C. (2017). *Analyse en composantes principales avec SPSS.* Université Catholique de Louvain-la-neuve. En ligne sur http://sites.uclouvain.be/selt/ressources/334103 (vidéo consultée le 18/07/19)

L'Hoiry, X. D., & Norris, C. (2015). The honest data protection officer's guide to enable citizens to exercise their subject access rights: Lessons from a ten-country european study. *International Data Privacy Law*, 5(3), 190-204. doi:10.1093/idpl/ipv009

Liu, C., Marchewka, J. T., Lu, J., & Yu, C. (2005). Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. *Information & Management, 42*(2), 289-304. doi:10.1016/j.im.2004.01.003

Lynskey, O. (2015). The foundations of EU data protection law. *Oxford: Oxford University Press*.

Macenaite, M., & Kosta, E. (2017). Consent for processing children's personal data in the EU: Following in US footsteps? *Information & Communications Technology Law*, 26(2), 146-197. doi:10.1080/13600834.2017.1321096

Manant, M., Rallet, A. & Rochelandet, F. (2018). Privacy et antitrust : des régulations contradictoires ou complémentaires ?. *Revue économique*, vol. 69(4), 647-667. https://www.cairn.info/revue-economique-2018-4-page-647.htm.

Manokha, I. (2018). The cambridge analytica scandal contextualized: Platform capital, surveillance, and data as a new 'fictitious commodity'. *Cultures Et Conflits, 109*(1), 30-59. doi:10.4000/conflits.19779

Merisavo, M., & Raulas, M. (2004). The impact of e-mail marketing on brand loyalty. *Journal of Product & Brand Management*, 13(7), 498-505. doi:10.1108/10610420410568435

Merton R.K. (1968), The Mathew effect in science, *Science*, 159, 3810, 56-63

Micheaux, A. L. (2011). Managing e-mail advertising frequency from the consumer perspective. *Journal of Advertising*, 40(4), 45-66. doi:10.2753/JOA0091-3367400404

Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing*, 12(2), 206-215. doi:10.1177/074391569101200206

Miyazaki, A. D., & Krishnamurthy, S. (2002). The journal of consumer affairs: Internet seals of approval: Effects on online privacy policies and consumer perceptions. *Family Economics and Nutrition Review*, 14(2), 99.

Mosco, V. (2014). To the Cloud: Big Data in a Turbulent World. *Paradigm Publishers.*

Mugnier, A. (2018). *Facebook : comprendre le scandale Cambridge Analytica*. Le Soir. En ligne sur https://www.lesoir.be/150181/article/2018-04-09/facebook-comprendre-le-scandale-cambridge-analytica (Consulté le 21/12/18)

Nairn, A., & Monkgol, D. (2007). Children and privacy online. *Journal of Direct, Data and Digital Marketing Practice*, 8(4), 294-308. doi:10.1057/palgrave.dddmp.4350063

Nature. (2018). Cambridge analytica controversy must spur researchers to update data ethics. , 555(7698), 559-560. doi:10.1038/d41586-018-03856-4

Ouellet, J. (2018). La fin de la satisfaction client à tout prix. *Gestion*, vol. 43(2), 72-75. doi:10.3917/riges.432.0072.

Papacharissi, Z., & Fernback, J. (2005). Online privacy and consumer protection: An analysis of portal privacy statements. *Journal of Broadcasting & Electronic Media*, 49(3), 259-281. doi:10.1207/s15506878jobem4903_1

Parlement Européen et Conseil de l'Union Européenne.(2016). Règlement Général sur la Protection des Données (RGPD). *Journal officiel de l'Union européenne*. En ligne sur https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679 (Document pdf consulté le 27/05/18)

Payne, A., & Frow, P. (2005). A strategic framework for customer relationship management. *Journal of Marketing*, 69(4), 167-176. doi:10.1509/jmkg.2005.69.4.167

Pernot, E. (2018). *Le droit à la portabilité des données dans le RGPD*. En ligne sur https://epernot.com/fr/droit-portabilite-des-donnees-rgpd/ (Consulté le 22/12/2018)

Pleyers, G. (2018). *Analyser, prédire et optimiser les réactions du consommateur LLSMS2024*. Université Catholique de Louvain-la-Neuve.

Priporas, C., Stylos, N., & Fotiadis, A. K. (2017). Generation Z consumers' expectations of interactions in smart retailing: A future agenda. *Computers in Human Behavior*, 77, 374-381. doi:10.1016/j.chb.2017.01.058

Raento, M. (2006). The data subject's right of access and to be informed in finland: An experimental study. *International Journal of Law and Information Technology*, 14(3), 390-409. doi:10.1093/ijlit/eal008

Rahman , M. H., & Kamrul Islam Shaon, S. M. (2015). A theoretical review of CRM effects on customer satisfaction and loyalty. *Central European Business Review*, 4(1), 23-36.

Reijmersdal, E. A. v., Boerman, S. C., Buijzen, M. A., & Rozendaal, E. (2017;2016;). This is advertising! effects of disclosing television brand placement on adolescents. *Journal of Youth and Adolescence*, 46(2), 328-342. doi:10.1007/s10964-016-0493-3

Reimers, V., Chao, C., & Gorman, S. (2016). Permission email marketing and its influence on online shopping. *Asia Pacific Journal of Marketing and Logistics*, 28(2), 308-322. doi:10.1108/APJML-03-2015-0037

Rifon, N. J., Larose, R., & CHOI, S. M. (2005;2006;). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *The Journal of Consumer Affairs*, 39(2), 339-362. doi:10.1111/j.1745-6606.2005.00018.x

Sabella, R. A., Patchin, J. W., & Hinduja, S. (2013). Cyberbullying myths and realities. *Computers in Human Behavior*, 29(6), 2703-2711. doi:10.1016/j.chb.2013.06.040

Schneble, C. O., Elger, B. S., & Shaw, D. (2018). The cambridge analytica affair and Internet-mediated research. *EMBO Reports*, 19(8), e46579-n/a. doi:10.15252/embr.201846579

Shah, H. (2017). The DeepMind debacle demands dialogue on data. *Nature*, 547(7663), 259-259. doi:10.1038/547259a

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, 19(1), 62-73. doi:10.1509/jppm.19.1.62.16949

Shepherd, I. D. H. (2005). From cattle and coke to charlie: Meeting the challenge of self marketing and personal branding. *Journal of Marketing Management*, 21(5-6), 589-606. doi:10.1362/0267257054307381

Simonnot, B. (2016). Place des moteurs de recherche dans l'éditorialisation du web. *Communication & Langages*, 188(2), 45-59. doi:10.4074/S0336150016012035

Soltani, Z., & Navimipour, N. J. (2016). Customer relationship management mechanisms: A systematic review of the state of the art literature and recommendations for future research. *Computers in Human Behavior*, 61, 667-688. doi:10.1016/j.chb.2016.03.008

SPF Economie. (2018). *Protection des données personnelles*. En ligne sur https://economie.fgov.be/fr/themes/line/securite-de-linformation/protection-des-donnees (Consulté le 20/12/18)

Stoughton, J. W., Thompson, L. F., & Meade, A. W. (2015). Examining applicant reactions to the use of social networking websites in pre-employment screening. *Journal of Business and Psychology, 30*(1), 73-88. doi:10.1007/s10869-013-9333-6

Such, J. M., Garcia-Fornes, A., & Botti, V. (2013). Automated buyer profiling control based on human privacy attitudes. *Electronic Commerce Research and Applications,* 12(6), 386-396. doi:10.1016/j.elerap.2013.05.001

Suen, H. (2018). How passive job candidates respond to social networking site screening. *Computers in Human Behavior*, 85, 396-404. doi:10.1016/j.chb.2018.04.018

Swaen, V. (2017). *Marketing research LLSMS2000.* Université Catholique de Louvain-la-neuve.

Teng, C., Tseng, F., & Chiang, D. M. (2006). Customer-capturing strategies: The way to replace existing technology characterized by network effects. *Technovation,* 26(12), 1384-1389. doi:10.1016/j.technovation.2005.08.005

Trusov, M., Ma, L., & Jamal, Z. (2016). Crumbs of the cookie: User profiling in customer-base analysis and behavioral targeting. *Marketing Science, 35*(3), 405-426. doi:10.1287/mksc.2015.0956

Tucker, C. (2019). Digital data, platforms and the usual [antitrust] suspects: Network effects, switching costs, essential facility. *Review of Industrial Organization, 54*(4), 683-694. doi:10.1007/s11151-019-09693-7

Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research*, 51(5), 546-562. doi:10.1509/jmr.10.0355

Turow, J. (2001). Family boundaries, commercialism, and the internet: A framework for research. *Journal of Applied Developmental Psychology*, 22(1), 73-86. doi:10.1016/S0193-3973(00)00067-8

Vandebosch, H., & Van Cleemput, K. (2009). Cyberbullying among youngsters: Profiles of bullies and victims. *New Media & Society,* 11(8), 1349-1371. doi:10.1177/1461444809341263

Vătămănescu, E., & Mănuc, D. (2013). Facebook self-(re)presentation and the employers' practice of using it as a recruitment tool. *Management Dynamics in the Knowledge Economy*

Wade, A., & Beran, T. (2011). Cyberbullying: The new era of bullying. *Canadian Journal of School Psychology*, 26(1), 44-61. doi:10.1177/0829573510396318

Wattal, S., Telang, R., Mukhopadhyay, T., & Boatwright, P. (2012). What's in a "name"? impact of use of customer information in E-mail advertisements. *Information Systems Research*, 23(3-part-1), 679-697. doi:10.1287/isre.1110.0384

White, T. B., Zahay, D. L., Thorbjørnsen, H., & Shavitt, S. (2008). Getting too personal: Reactance to highly personalized email solicitations. *Marketing Letters*, 19(1), 39-50. doi:10.1007/s11002-007-9027-9

Wilkey, A. (2012). How to realize the benefits of trigger-based marketing. *Customer*, 31(4), 20.

World Bank Open Data. (2018). *Population , male (% of total population)*. En ligne sur https://data.worldbank.org/indicator/SP.POP.TOTL.MA.ZS (Consulté le 12/07/19)

Xingan, L. (2006). E-marketing, unsolicited commercial E-mail, and legal solutions. *Webology*, 3(1), 23.

Yeh, C. (2018). Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers. *Telecommunications Policy*, *42*(4), 282-292. doi:10.1016/j.telpol.2017.12.001

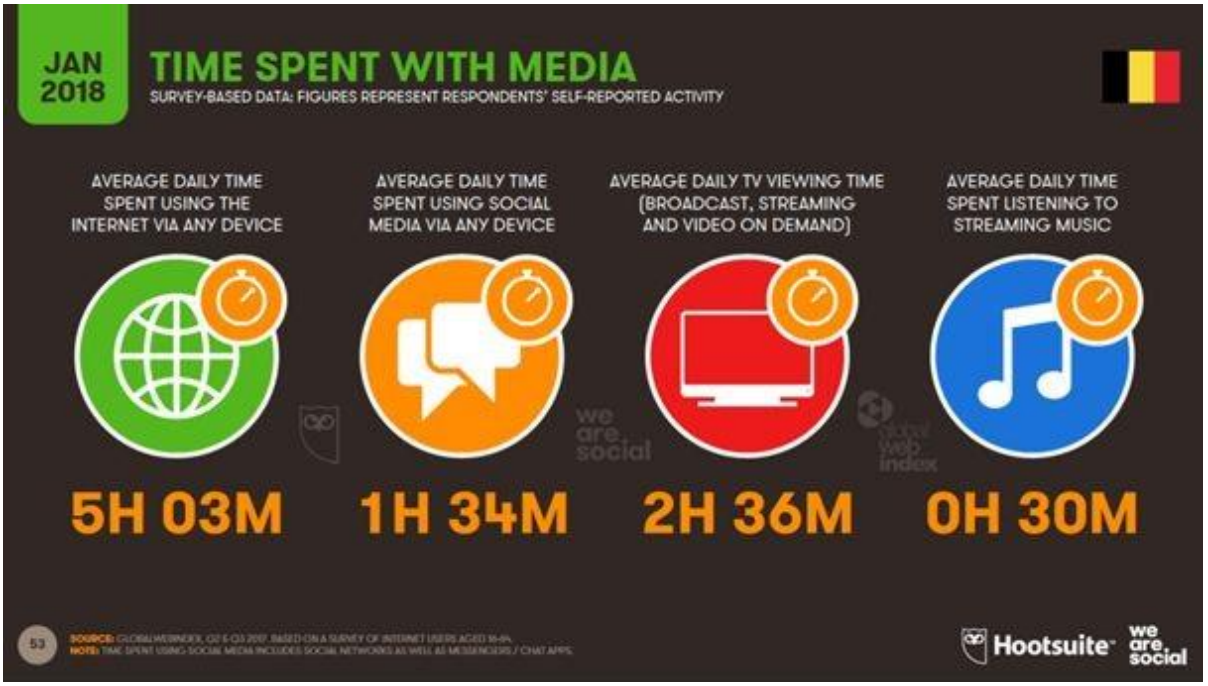
Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk-benefit appraisal approach. *Journal of Broadcasting & Electronic Media*, 49(1), 86-110. doi:10.1207/s15506878jobem4901_6

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *The Journal of Consumer Affairs*, 43(3), 389-418. doi:10.1111/j.1745-6606.2009.01146.x

Zahay, D., Peltier, J., & Krishen, A. S. (2012). Building the foundation for customer data quality in CRM systems for financial services firms. *Journal of Database Marketing and Customer Strategy Management*, 19(1), 5-16. doi:10.1057/dbm.2012.6

Annexes

Annexe 1 : Time spent with media (source : GlobalWebIndex)



Annexe 2 : Questionnaire en ligne (source : notre enquête)

L'impact du RGPD sur la confiance des consommateurs

Bonjour, je suis étudiant en dernière année de Master à la Louvain School of Management et mon mémoire porte sur l'impact du RGPD sur la confiance des consommateurs. Le Règlement Général sur la Protection des Données (RGPD ou de l'anglais GDPR), entré en vigueur le 25 mai 2018, vise à donner aux citoyens de l'union européenne davantage de contrôle et de visibilité sur leurs données personnelles. Ainsi, les questions qui vont suivre auront pour but principal d'identifier votre degré de confiance quant au partage de vos données personnelles au sein d'un monde de plus en plus connecté. Il n'y a ni bonne, ni mauvaise réponse. La confidentialité de vos réponses est assurée et seules les données agrégées seront étudiées. Les finalités du traitement des réponses auront pour pure vocation la recherche scientifique et non un but commercial.

*Obligatoire

1. **Saviez-vous qu'il était possible de transférer l'intégralité de vos données personnelles vers un autre service numérique ?** *

Une seule réponse possible.

- ◯ Oui
- ◯ Non

2. **Je comprends l'énoncé suivant : "Le droit à la portabilité offre la possibilité de récupérer une partie de vos données dans un format lisible par machine. Libre à vous de stocker ailleurs ces données portables ou de les transmettre facilement d'un système à un autre, en vue d'une réutilisation à d'autres fins."** *

Une seule réponse possible.

	1	2	3	4	5	6	7	
Pas du tout d'accord	◯	◯	◯	◯	◯	◯	◯	Tout à fait d'accord

3. **J'apprécie la réutilisation de mes données auprès d'un autre service numérique** *

Une seule réponse possible.

	1	2	3	4	5	6	7	
Pas du tout d'accord	◯	◯	◯	◯	◯	◯	◯	Tout à fait d'accord

Section 2/8

4. **Saviez-vous qu'il était possible de demander à un site de e-commerce la mise à jour de vos données personnelles ?** *

Une seule réponse possible.

- Oui
- Non

5. **Je comprends l'énoncé suivant : "La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes. Compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées."** *

Une seule réponse possible.

	1	2	3	4	5	6	7	
Pas du tout d'accord	◯	◯	◯	◯	◯	◯	◯	Tout à fait d'accord

6. **J'apprécie de pouvoir mettre à jour mes données personnelles auprès d'un responsable de traitement** *

Une seule réponse possible.

	1	2	3	4	5	6	7	
Pas du tout d'accord	◯	◯	◯	◯	◯	◯	◯	Tout à fait d'accord

Section 3/8

7. **Saviez-vous qu'il était possible de demander l'effacement des données collectées alors que vous étiez encore mineur à l'époque de la collecte?** *

Une seule réponse possible.

- ◯ Oui
- ◯ Non

8. **Je comprends l'énoncé suivant : "La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant."** *

Une seule réponse possible.

	1	2	3	4	5	6	7	
Pas du tout d'accord	◯	◯	◯	◯	◯	◯	◯	Tout à fait d'accord

9. **J'apprécie de pouvoir demander la suppression des données collectées à mon égard** *

Une seule réponse possible.

	1	2	3	4	5	6	7	
Pas du tout d'accord	◯	◯	◯	◯	◯	◯	◯	Tout à fait d'accord

Section 4/8

10. **Connaissiez-vous l'existence de ce logo ?** *

Une seule réponse possible.

- ◯ Oui
- ◯ Non

11. **Je comprends la signification du logo, visible sur certains sites internet** *

Une seule réponse possible.

	1	2	3	4	5	6	7	
Pas du tout d'accord	◯	◯	◯	◯	◯	◯	◯	Tout à fait d'accord

12. **La présence de ce logo renforce ma disposition à partager mes informations personnelles** *

Une seule réponse possible.

	1	2	3	4	5	6	7	
Pas du tout d'accord	◯	◯	◯	◯	◯	◯	◯	Tout à fait d'accord

Section 5/8

13. **Saviez-vous qu'il était possible d'accéder à vos données personnelles détenues par un réseau social ?** *

Une seule réponse possible.

- ◯ Oui
- ◯ Non

14. **Je comprends l'énoncé suivant : "La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel."** *

Une seule réponse possible.

	1	2	3	4	5	6	7	
Pas du tout d'accord	◯	◯	◯	◯	◯	◯	◯	Tout à fait d'accord

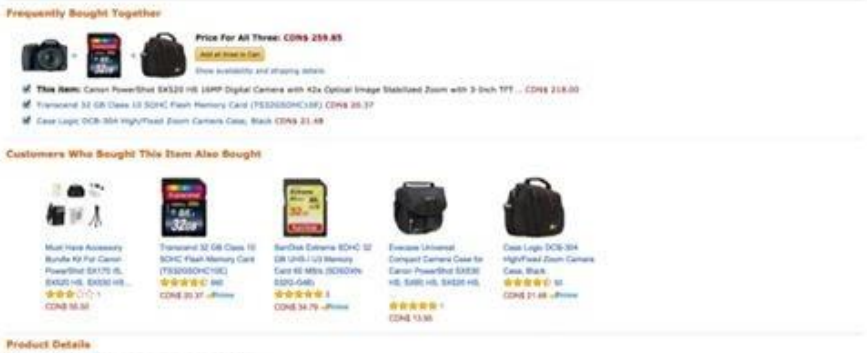
15. **J'apprécie de connaître les données qu'un organisme détient sur moi** *

Une seule réponse possible.

	1	2	3	4	5	6	7	
Pas du tout d'accord	◯	◯	◯	◯	◯	◯	◯	Tout à fait d'accord

Section 6/8

16. **Connaissiez-vous les activités de cross-selling, entendues au sens de vente de produits complémentaires?** *



Une seule réponse possible.

- ◯ Oui
- ◯ Non

17. **Je comprends l'énoncé suivant : "La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant, y compris au profilage basé sur ces données."** *

Une seule réponse possible.

	1	2	3	4	5	6	7	
Pas du tout d'accord	◯	◯	◯	◯	◯	◯	◯	Tout à fait d'accord

18. **J'apprécie de pouvoir m'opposer à tout moment à l'utilisation faites de mes données** *

Une seule réponse possible.

	1	2	3	4	5	6	7	
Pas du tout d'accord	◯	◯	◯	◯	◯	◯	◯	Tout à fait d'accord

Section 7/8

19. **Saviez-vous qu'il était possible de demander à un réseau social la conservation des preuves de harcèlement en ligne ?** *

Une seule réponse possible.

- ◯ Oui
- ◯ Non

20. **Je comprends l'énoncé suivant : "La personne concernée a le droit de demander à un organisme de geler temporairement l'utilisation de ses données personnelles."** *

Une seule réponse possible.

	1	2	3	4	5	6	7	
Pas du tout d'accord	◯	◯	◯	◯	◯	◯	◯	Tout à fait d'accord

21. **J'apprécie la possibilité de pouvoir geler temporairement l'utilisation de certaines de mes données** *

Une seule réponse possible.

	1	2	3	4	5	6	7	
Pas du tout d'accord	◯	◯	◯	◯	◯	◯	◯	Tout à fait d'accord

Section 8/8

22. **Quel est votre âge ?** *

Une seule réponse possible.

- ◯ 10-20 ans
- ◯ 21-30 ans
- ◯ 31-40 ans
- ◯ 41-50 ans
- ◯ 51 et +

23. **Quel est votre niveau d'étude ?** *
Une seule réponse possible.

- ◯ Enseignement primaire - secondaire
- ◯ Bachelier
- ◯ Master - Doctorat
- ◯ Autre

24. **Quel est votre sexe ?** *
Une seule réponse possible.

- ◯ Masculin
- ◯ Féminin

25. **Pensez-vous être "accro" à votre smartphone ?** *
Une seule réponse possible.

- ◯ Oui
- ◯ Non

26. **Habituellement, êtes-vous réticent à l'idée de partager vos informations personnelles ?** *
Une seule réponse possible.

- ◯ Oui
- ◯ Non

27. **Qu'avez-vous pensé de ce questionnaire ?**

_____

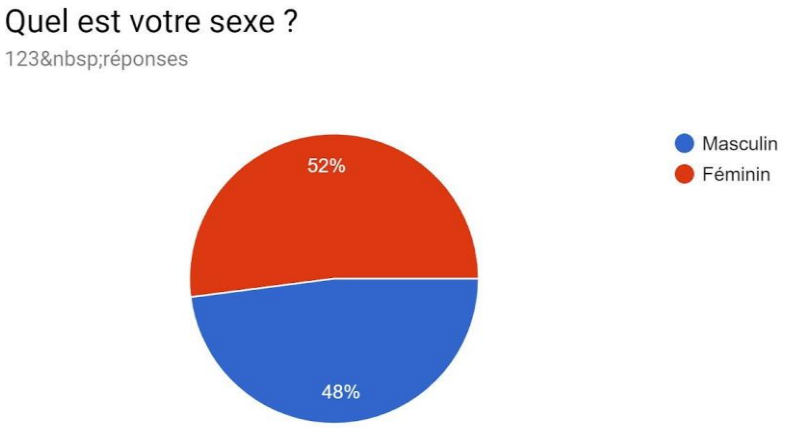
Fourni par
Google Forms

Annexe 3 : Dictionnaire des variables

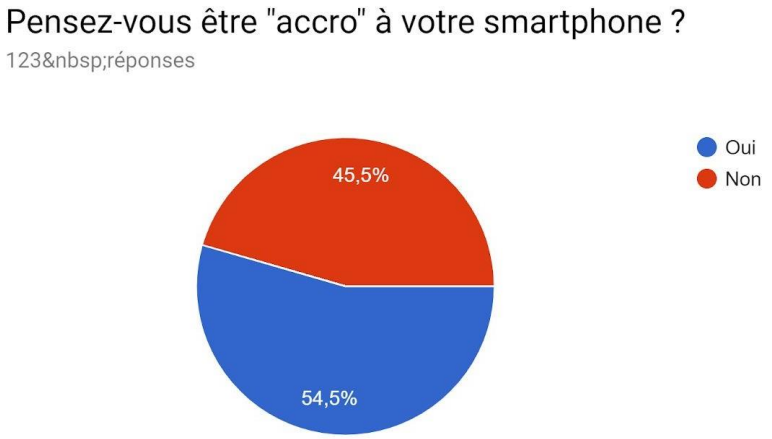
Question N°	Nom de la variable	Modalité
1	Portabilite	0 = Non ; 1 = Oui
2	Comprehensionportabilite	1=Pas du tout d'accord à 7=Tout à fait d'accord
3	Appreciationportabilite	1=Pas du tout d'accord à 7=Tout à fait d'accord
4	Rectification	0 = Non ; 1 = Oui
5	Comprehensionrectification	1=Pas du tout d'accord à 7=Tout à fait d'accord
6	Appreciationrectification	1=Pas du tout d'accord à 7=Tout à fait d'accord
7	Effacement	0 = Non ; 1 = Oui
8	Comprehensioneffacement	1=Pas du tout d'accord à 7=Tout à fait d'accord
9	Appreciationeffacement	1=Pas du tout d'accord à 7=Tout à fait d'accord
10	Existencelogo	0 = Non ; 1 = Oui
11	Comprehensionlogo	1=Pas du tout d'accord à 7=Tout à fait d'accord
12	Renforcementlogo	1=Pas du tout d'accord à 7=Tout à fait d'accord
13	Acces	0 = Non ; 1 = Oui
14	Compréhensionacces	1=Pas du tout d'accord à 7=Tout à fait d'accord
15	Appreciationaccces	1=Pas du tout d'accord à 7=Tout à fait d'accord
16	Crossselling	0 = Non ; 1 = Oui

17	Comprehensioncrossselling	1=Pas du tout d'accord à 7=Tout à fait d'accord
18	Appreciationcrossselling	1=Pas du tout d'accord à 7=Tout à fait d'accord
19	Limitation	0 = Non ; 1 = Oui
20	Comprehensionlimitation	1=Pas du tout d'accord à 7=Tout à fait d'accord
21	Appreciationlimitation	1=Pas du tout d'accord à 7=Tout à fait d'accord
22	Age	1=10-20 ans ; 2=21-30 ans ; 3=31-40 ans ; 4=41-50 ans ; 5=51 et +
23	Niveaudétude	1=Primaire–secondaire ; 2=Bachelier ; 3=Master-Doctorat ; 0=Autre
24	Sexe	0=Masculin ; 1=Féminin
25	Accro	0 = Non ; 1 = Oui
26	Reticence	0 = Non ; 1 = Oui
27	Avis	
	Age regroupé	0=10-30 ans ; 1=31 et +
	CompTot	= Comprehensionmisejour + Comprehensioneffacement + Comprehensionacces + Comprehensioncrosselling
	AppTot	= Appreciationeffacement + Appreciationacces + Appreciationcrosselling + Appreciationlimitation
	PartageLogo	0=Renforcementlogo(1-3) ; 1= Renforcementlogo(4-7)
	Connaissance	Portabilité + Rectification + Effacement + Existencelogo + Acces + Crossselling + limitation

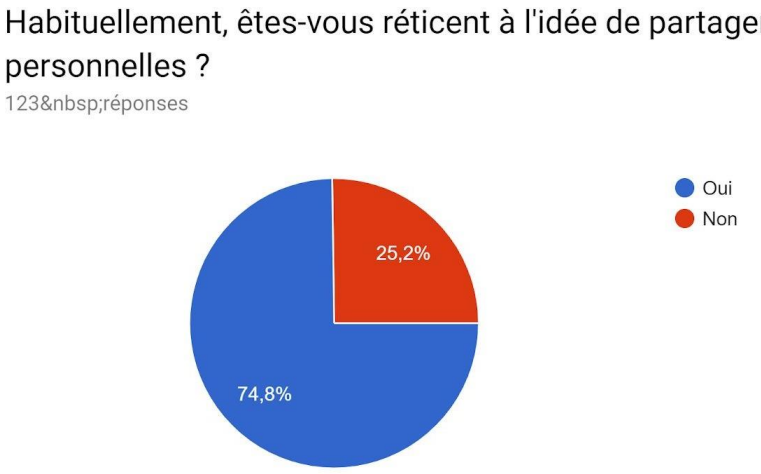
Annexe 4 : Répartition des répondants selon le sexe (source : notre enquête)



Annexe 5: Répartition des répondants selon l'addiction au smartphone (source : notre enquête)



Annexe 6 : Répartition des répondants selon la réticence habituelle au partage d'informations personnelles (source : notre enquête)



Annexe 7 : alpha de Cronbach, échelle de compréhension (source : SPSS)

Statistiques de fiabilité de l'échelle de compréhension

Alpha de Cronbach	Alpha de Cronbach basé sur des éléments standardisés	Nombre d'éléments
,747	,752	4

Annexe 8 : Moyenne agrégée de compréhension du RGPD (source : SPSS)

Statistiques d'échelle de compréhension

Moyenne	Variance	Ecart type	Nombre d'éléments
23,07	19,455	4,411	4

Annexe 9 : alpha de Cronbach, échelle d'appréciation (source : SPSS)

Statistiques de fiabilité de l'échelle d'appréciation

Alpha de Cronbach	Alpha de Cronbach basé sur des éléments standardisés	Nombre d'éléments
,546	,555	4

Annexe 10 : Moyenne agrégée d'appréciation du RGPD (source : SPSS)

Statistiques d'échelle d'appréciation

Moyenne	Variance	Ecart type	Nombre d'éléments
25,75	7,633	2,763	4

Annexe 11 : Test binomial sur la connaissance de la portabilité (source : SPSS)

Test binomial

		Catégorie	Effectif	Proportion observée	Proportion testée	p-value
Portabilité	Groupe 1	Non	60	,49	,50	,857
	Groupe 2	Oui	63	,51		
	Total		123	1,00		

Annexe 12 : Test T sur la compréhension de la portabilité (source : SPSS)

Test sur échantillon unique

	N	Moyenne	p-value
Comprehensionportabilite	123	4,62	,000

Annexe 13 : Test T sur l'appréciation de la portabilité (source : SPSS)

Test sur échantillon unique

	N	Moyenne	p-value
Appreciationportabilite	123	3,38	,001

Annexe 14 : Test binomial sur la connaissance de la rectification (source : SPSS)

Test binomial

		Catégorie	N	Proportion observée	Proportion testée	p-value
Rectification	Groupe 1	Non	45	,37	,50	,004
	Groupe 2	Oui	78	,63		
	Total		123	1,00		

Annexe 15 : Test T sur la compréhension de la rectification (source : SPSS)

Test sur échantillon unique

	N	Moyenne	p-value
Comprehensionrectification	123	5,77	,000

Annexe 16 : Test T sur l'appréciation de la rectification (source : SPSS)

Test sur échantillon unique

	N	Moyenne	p-value
Appreciationrectification	123	5,28	,000

Annexe 17 : Test binomial sur la connaissance de l'effacement (source : SPSS)

Test binomial

		Catégorie	N	Proportion observée	Proportion testée	p-value
Effacement	Groupe 1	Non	94	,76	,50	,000
	Groupe 2	Oui	29	,24		
	Total		123	1,00		

Annexe 18 : Test T sur la compréhension de l'effacement (source : SPSS)

Test sur échantillon unique

	N	Moyenne	p-value
Comprehensioneffacement	123	6,29	,000

Annexe 19 : Test T sur l'appréciation de l'effacement (source : SPSS)

Test sur échantillon unique

	N	Moyenne	p-value
Appreciationeffacement	123	6,52	,000

Annexe 20 : Test binomial sur la connaissance du label RGPD (source : SPSS)

Test binomial

		Catégorie	N	Proportion observée	Proportion testée	p-value
Existencelogo	Groupe 1	Non	91	,74	,50	,000
	Groupe 2	Oui	32	,26		
	Total		123	1,00		

Annexe 21 : Test T sur la compréhension du label RGPD (source : SPSS)

Test sur échantillon unique

	N	Moyenne	p-value
Comprehensionlogo	123	4,98	,000

Annexe 22 : Test T sur l'augmentation de la propension du partage de données stimulée par le label RGPD (source : SPSS)

Test sur échantillon unique

	N	Moyenne	p-value
Renforcementlogo	123	4,02	,890

Annexe 23 : Tableau de contingence Réticence * Partage label (source : SPSS)

Tableau croisé Reticence * PartageLogo

			PartageLogo		
			Non	Oui	Total
Reticence	Non	Effectif	13	18	31
		% dans Reticence	41,9%	58,1%	100,0%
	Oui	Effectif	35	57	92
		% dans Reticence	38,0%	62,0%	100,0%
Total		Effectif	48	75	123
		% dans Reticence	39,0%	61,0%	100,0%

Annexe 24 : Test du Chi-carré entre la réticence et le partage stimulé par le label (source : SPSS)

Tests du khi-carré

	Valeur	ddl	p-value
khi-carré de Pearson	,148[a]	1	,701
N d'observations valides	123		

a. 0 cellules (0,0%) ont un effectif théorique inférieur à 5. L'effectif théorique minimum est de 12,10.

Annexe 25 : Test binomial sur la connaissance de l'accès (source : SPSS)

Test binomial

		Catégorie	N	Proportion observée	Proportion testée	p-value
Acces	Groupe 1	Non	40	,33	,50	,000
	Groupe 2	Oui	83	,67		
	Total		123	1,00		

Annexe 26 : Test T sur la compréhension de l'accès (source : SPSS)

Test sur échantillon unique

	N	Moyenne	p-value
Comprehensionacces	123	5,33	,000

Annexe 27 : Test T sur l'appréciation de l'accès (source : SPSS)

Test sur échantillon unique

	N	Moyenne	p-value
Appreciationacces	123	6,33	,000

Annexe 28 : Test binomial sur la connaissance du cross-selling (source : SPSS)

Test binomial

		Catégorie	N	Proportion observée	Proportion testée	p-value
Crosssellin g	Groupe 1	Non	39	,32	,50	,000
	Groupe 2	Oui	84	,68		
	Total		123	1,00		

Annexe 29 : Test T sur la compréhension de l'opposition (source : SPSS)

Test sur échantillon unique

	N	Moyenne	p-value
Comprehensioncrosssellin g	123	5,67	,000

Annexe 30 : Test T sur l'appréciation de l'opposition (source : SPSS)

Test sur échantillon unique

	N	Moyenne	p-value
Appreciationcrossselli ng	123	6,56	,000

Annexe 31 : Test binomial sur la connaissance de la limitation (source : SPSS)

Test binomial

		Catégorie	N	Proportion observée	Proportion testée	p-value
Limitation	Groupe 1	Non	99	,80	,50	,000
	Groupe 2	Oui	24	,20		
	Total		123	1,00		

Annexe 32 : Test T sur la compréhension de la limitation (source : SPSS)

Test sur échantillon unique

	N	Moyenne	p-value
Comprehensionlimitation	123	6,10	,000

Annexe 33 : Test T sur l'appréciation de la limitation (source : SPSS)

Test sur échantillon unique

	N	Moyenne	p-value
Appreciationlimitation	123	6,33	,000

Annexe 34 : Test T pour comparer la compréhension de l'effacement suivant l'addiction (source : SPSS)

Test pour échantillons indépendants

	Accro	N	Moyenne	p-value égalité des variances	p-value comparaison de moyenne
Comprehensioneffacement	Non	56	6,52	,065	,043
	Oui	67	6,10		

Annexe 35 : Test T pour comparer la compréhension du label suivant l'addiction (source : SPSS)

Test pour échantillons indépendants

	Accro	N	Moyenne	p-value égalité des variances	p-value comparaison de moyenne
Comprehensioneffacement	Non	56	5,54	,009	,004
	Oui	67	4,52		

Annexe 36 : Compréhension non significative par groupe d'addiction (source : SPSS)

		Test de Levene sur l'égalité des variances	Test t pour égalité des moyennes
		Sig.	Sig. (bilatéral)
Comprehensionportabilite	Hypothèse de variances égales	,864	,223
Comprehensionrectification	Hypothèse de variances égales	,130	,928
Compréhensionacces	Hypothèse de variances égales	,165	,727
Comprehensioncrossselling	Hypothèse de variances égales	,898	,115
Comprehensionlimitation	Hypothèse de variances égales	,563	,121

Annexe 37 : Test T pour comparer la compréhension des outils juridiques suivant l'âge (source : SPSS)

		Test de Levene sur l'égalité des variances Sig.	Test t pour égalité des moyennes Sig. (bilatéral)
Comprehensionportabilite	Hypothèse de variances égales	,023	,732
	Hypothèse de variances inégales		,741
Comprehensionrectification	Hypothèse de variances égales	,333	,353
Comprehensioneffacement	Hypothèse de variances égales	,553	,511

Comprehensionlogo	Hypothèse de variances égales	,143	,230
Compréhensionacces	Hypothèse de variances égales	,179	,615
Comprehensioncrossselling	Hypothèse de variances égales	,498	,582
Comprehensionlimitation	Hypothèse de variances égales	,393	,895

Annexe 38 : Test T pour comparer la compréhension des outils juridiques suivant le sexe (source : SPSS)

		Test de Levene sur l'égalité des variances	Test t pour égalité des moyennes
		Sig.	Sig. (bilatéral)
Comprehensionportabilite	Hypothèse de variances égales	,920	,110
	Hypothèse de variances inégales		,111
Comprehensionrectification	Hypothèse de variances égales	,496	,439
Comprehensioneffacement	Hypothèse de variances égales	,929	,966
	Hypothèse de variances inégales		,966
Comprehensionlogo	Hypothèse de variances égales	,890	,058
	Hypothèse de variances inégales		,059
Compréhensionacces	Hypothèse de variances égales	,342	,680

Comprehensioncrossselling	Hypothèse de variances égales	,922	,540
	Hypothèse de variances inégales		,540
Comprehensionlimitation	Hypothèse de variances égales	,338	,271

Annexe 39 : Anova pour comparer la compréhension des outils juridiques suivant le niveau d'éducation (source : SPSS)

ANOVA

	Test d'homogénéité des variances p-value	Test de comparaison de moyenne p-value
Comprehensionportabilite	,779	,541
Comprehensioneffacement	,140	,425
Comprehensionlogo	,703	,152
Compréhensionacces	,250	,230
Comprehensionlimitation	,086	,591

Annexe 40 : Test de Welch pour comparer la compréhension de la rectification et de l'opposition suivant le niveau d'éducation (source : SPSS)

Tests robustes d'égalité des moyennes

		Test d'homogénéité des variances p-value	Test de comparaison de moyenne p-value.
Comprehensionrectification	Welch	,002	,173
Comprehensioncrossselling	Welch	,005	,494

Annexe 41 : Test T pour comparer l'appréciation de l'opposition suivant l'addiction (source : SPSS)

Test des échantillons indépendants

	Accro	N	Moyenne	Test sur l'égalité des variances p-value	Test pour l'égalité des moyennes p-value
Appreciationcrossselling	**Non**	**56**	**6,75**	**,004**	**,042**
	Oui	**67**	**6,40**		

Annexe 42 : Appréciation non significative selon l'addiction au smartphone (source : SPSS)

Test des échantillons indépendants

		Test de Levene sur l'égalité des variances p-value	Test t pour égalité des moyennes p-value
Appreciationportabilite	Hypothèse de variances égales	,193	,487
Appreciationrectification	Hypothèse de variances égales	,429	,498
Appreciationeffacement	Hypothèse de variances égales	,717	,868
Renforcementlogo	Hypothèse de variances égales	,074	,148
Appreciationaccces	Hypothèse de variances égales	,011	,272
	Hypothèse de variances inégales		,296
Appreciationlimitation	Hypothèse de variances égales	,124	,071

Annexe 43 : Test T pour comparer le renforcement label suivant l'âge (source : SPSS)

Test pour échantillons indépendants

	Age regroupé	N	Moyenne	Test sur l'égalité des variances p-value	Test pour l'égalité des moyennes p-value
Renforcementlogo	10-30 ans	72	4,43	,614	,006
	31 et +	51	3,45		

Annexe 44 : Appréciation non significative des autres outils juridiques suivant l'âge (source : SPSS)

Test des échantillons indépendants

		Test de Levene sur l'égalité des variances Sig.	Test t pour égalité des moyennes Sig. (bilatéral)
Appreciationportabilite	Hypothèse de variances égales	,771	,812
Appreciationrectification	Hypothèse de variances égales	,407	,283
Appreciationeffacement	Hypothèse de variances égales	,077	,385
Appreciationaccces	Hypothèse de variances égales	,015	,147
	Hypothèse de variances inégales		,182
Appreciationcrossselling	Hypothèse de variances égales	,033	,171

	Hypothèse de variances inégales		,144
Appreciationlimitation	Hypothèse de variances égales	,065	,113

Annexe 45 : Test T pour comparer l'appréciation des outils juridiques suivant le sexe (source : SPSS)

Test des échantillons indépendants

		Test de Levene sur l'égalité des variances	Test t pour égalité des moyennes
		Sig.	Sig. (bilatéral)
Renforcementlogo	Hypothèse de variances égales	,255	,126
Appreciationportabilite	Hypothèse de variances égales	,021	,429
	Hypothèse de variances inégales		,433
Appreciationrectification	Hypothèse de variances égales	,273	,255
Appreciationeffacement	Hypothèse de variances égales	,027	,225
	Hypothèse de variances inégales		,220
Appreciationaccces	Hypothèse de variances égales	,149	,295
Appreciationcrossselling	Hypothèse de variances égales	,315	,597
Appreciationlimitation	Hypothèse de variances égales	,132	,203

Annexe 46 : Anova pour comparer l'appréciation de la rectification suivant le niveau d'éducation (source : SPSS)

ANOVA

Appreciationrectification

	N	Moyenne	Test d'homogénéité des variances p-value	Test de comparaison de moyenne p-value
Autre	4	4,25	,277	,006
Primaire-Secondaire	4	2,75		
Bachelier	46	5,41		
Master-Doctorat	69	5,41		
Total	123	5,28		

Annexe 47 : Appréciation non significative de la portabilité, de l'opposition, de la limitation et du label (source : SPSS)

ANOVA

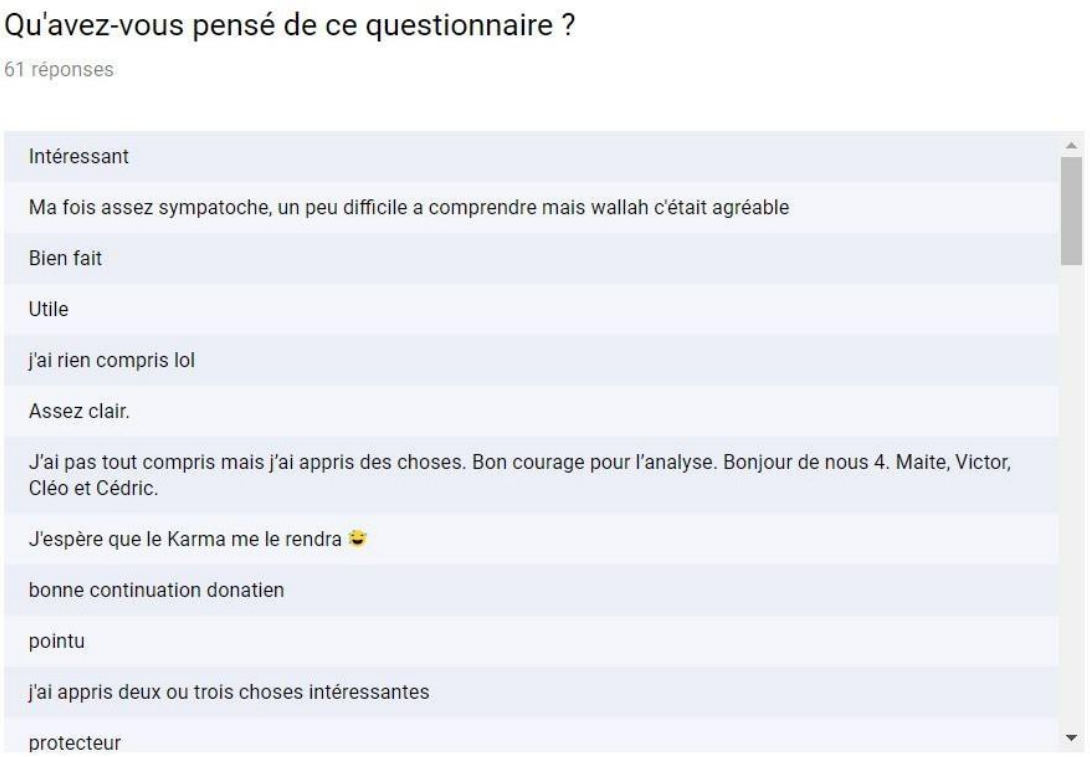
	Test d'homogénéité des variances p-value	Test de comparaison de moyenne p-value
Appreciationportabilite	,052	,955
Appreciationcrossselling	,091	,658
Appreciationlimitation	,626	,678
Renforcementlogo	,324	,348

Annexe 48 : Test de Welch pour comparer l'appréciation de l'effacement et de l'accès suivant le niveau d'éducation (source : SPSS)

Tests robustes d'égalité des moyennes

		Test d'homogénéité des variances p-value	Test de comparaison de moyenne p-value.
Appreciationeffacement	Welch	,008	.
Appreciationacces	Welch	,007	,819

Annexe 49 : Réponses à la question ouverte facultative (source : notre enquête)



Qu'avez-vous pensé de ce questionnaire ?

61 réponses

Intéressant ! On apprend pas mal de choses qui peuvent être possible pour nous en tant que citoyens. Des informations qui ne sont pas naturellement communiquées et qui devraient pourtant l'être davantage.

Interessant !!

Top. Bonne chance

Rien à redire. Clair et pas trop long ... mais où iront nos données personnelles issues de nos réponses ?

Pas mal du tout :-) bonne chance!

J'ai envie de me méfier davantage sur les informations que je communique car je me'rends compte que je n'en fais pas toujours attention aux phrases hyper complexes utilisées dans ce domaine

Mémoire interessant

M'a permis de m' informer sur ce que je ne connaissais pas

D'actualité et très intéressant pour les " méfiants du net"

Très fluide pas trop long et très clair

Avec un questionnaire pareil, je pense que tu cours tout droit vers une grande distinction à ton mémoire, la bise

Qu'avez-vous pensé de ce questionnaire ?

61 réponses

Instructif.

J'ai appris des choses

Très intéressant et instructif

Très clair, informatif

Instructif

Intéressant et instructif

J'ai eu du mal à répondre aux trois premières questions, ça n'était pas clair. Bonne chance pour ton mémoire!

Complet et bien pensé

Excellent

utile, intelligent et bien ficelé

L'impact du RGPD sur la confiance des consommateurs est un sujet intéressant.

révélateur

Qu'avez-vous pensé de ce questionnaire ?

61 réponses

très clair

ce questionnaire reprend les questions à se poser en matière du traitement des données personnelles. Nous savons tous que nos données sont utilisées par tous. nous ignorons souvent comment on peut éviter et se protéger.

Intéressant que l'avis du consommateur soit demandé ...

Je n'ai pas tout compris mais ça à l'air intéressant.

Nice!

intéressant

Ça montre que tout le monde saura tout de tout le monde et qu'il n'y aura plus de vie privée plus tard.

Bon questionnement sur un sujet très peu connu

Questions parfois pas très claires

Questions pas toujours clairs car dans les faits, c'est compliqué d'obtenir nos informations. On est plus manipulé qu'autre chose et n'avons aucun moyen de contrôle sur l'utilisation réelle de nos données

Étrange au niveau des énoncés

Qu'avez-vous pensé de ce questionnaire ?

61 réponses

Il est plutôt rare de trouver des questions comme celle-ci à la fin du questionnaire. Elle est pourtant très intéressante. C'est un questionnaire rapide, bien orthographié et facile de compréhension. Peut-être mettre un lien pour les répondants (en fin d'enquête) avec plus d'infos au sujet des RGPD?

Il m'a appris de nombreuses informations qui me paraissent essentielles et que pourtant je ne connaissais pas. Questionnaire facile et rapide

Très intéressant

Instructif, ne connaissant pas ces sujets liés aux droits juridiques, possibilités des demandes sur le net.

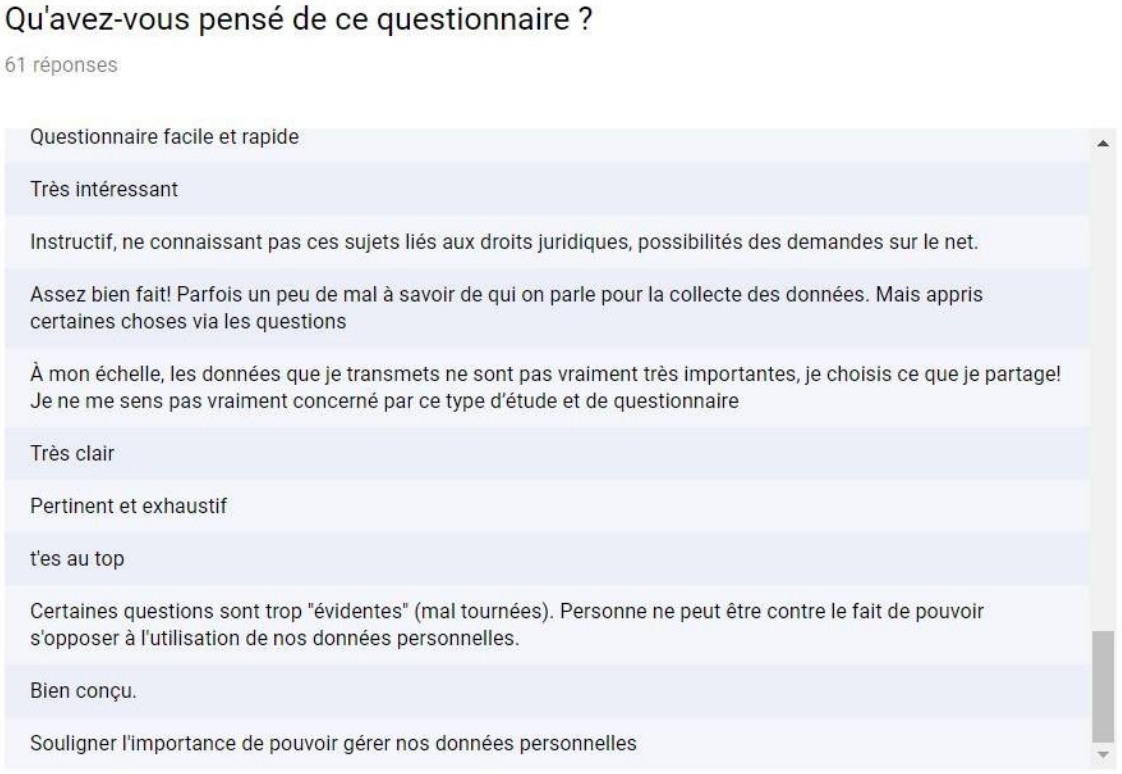
Assez bien fait! Parfois un peu de mal à savoir de qui on parle pour la collecte des données. Mais appris certaines choses via les questions

À mon échelle, les données que je transmets ne sont pas vraiment très importantes, je choisis ce que je partage! Je ne me sens pas vraiment concerné par ce type d'étude et de questionnaire

Très clair

Pertinent et exhaustif

t'es au top



Annexe 50 : Rule of thumb (source : Marketing research LLSMS2000)

LOUVAIN-LA-NEUVE | BRUXELLES | MONS | TOURNAI | CHARLEROI | NAMUR
Place des Doyens, 1 bte L2.01.01, 1348 Louvain-la-Neuve, Belgique | **www.uclouvain.be/lsm**