SSH3501 - ÉTHIQUE APPLIQUÉE À L'INGÉNIERIE

AUTOMNE 2021

ISMAIL BAKKOURI – 1954157

DE2 :

Est-il éthiquement et moralement acceptable que les entreprises collectent les données personnelles pour garder leurs services gratuits ?

GROUPE : 01

PRÉSENTÉ À :

GABRIEL BARIL

LE 19 OCTOBRE 2021

I) Introduction (résumé du DE1)

Lors de la présentation du DE1, il était question des enjeux relatifs à la collecte de données personnelles que les grandes multinationales telles que Facebook, Google ou encore Amazon font pour permettre de garder leur service gratuit. En effet, les multinationales font une collecte massive de données que les utilisateurs communiquent (parfois inconsciemment) sur leurs services et sauvegardent ainsi diverses informations détaillées concernant la vie des individus, comme le nom, adresse, numéro de téléphone, photos, ou encore des données très personnelles relatives aux gouts et aux préférences de l'individu. La collecte de données leur permet ainsi de à certaines compagnies de revendre ces données personnelles afin d'en tirer profit, et à d'autre, de les analyser pour permettre de proposer du contenu personnalisé, plus susceptible d'intéresser les utilisateurs des services proposés, afin de maximiser leurs profits au détriment de tout principe moral ou éthique. Les informations avec lesquelles il devient possible de retracer en détail la vie de quelqu'un deviennent juste des données à monnayer de la façon la plus rentable possible, et ce, bien souvent, dans l'ignorance la plus totale des principaux concernés.

Ces entreprises dépensent des millions de dollars en frais d'ingénieurs spécialisés au développement d'algorithmes informatiques, afin d'automatiser le processus de collecte de ces données et de l'optimiser au maximum. La problématique étant que l'écrasante majorité des utilisateurs de ces services ne savent pas que toutes les actions qu'ils réalisent sur leurs applications sont scrutées à leur insu, et connaissent encore moins l'étendue de cette scrutation. En effet, certains services dits gratuits comme le fameux « Google maps », que tout le monde trouve très pratique et indispensable, collectent par exemple toutes les données relatives aux déplacements effectués par l'utilisateur du service. En consultant ces données, il est donc possible de connaître en détail l'historique des allées et venues de quelqu'un [1]. Il en est de même pour les utilisateurs de Facebook qui va même jusqu'à collecter les données des utilisateurs même quand ceux-ci ne sont pas connectés sur le réseau social, ou à les extraire l'information à partir des conversations privées que l'utilisateur a avec ses amis [2].

En bref, il est clair que tout cela impose plusieurs dilemmes éthiques quant à cette collecte sans le consentement des principaux concernés ainsi que la zone d'ombre concernant de la monétisation de ces informations.

II) Exploration du sujet

a) Incertitudes

La collecte de données personnelles est un sujet encore méconnu de la population qui présente de nombreux éléments incompris. Il y'a en effet plusieurs questions à clarifier. Premièrement, est-ce que les données collectées sont accessibles par n'importe qui? Où y'a-t-il des sécurités qui empêchent l'accès aux données? Cette question a été explorée en profondeur par plusieurs chercheurs dans un article scientifique de l'université allemande Leibniz Hannover. Ces derniers ont analysé les risques que peuvent encourir les données personnelles que les utilisateurs des services informatiques mettent en ligne parfois sans avoir conscience des implications que cela peut avoir. Les chercheurs ont analysé un jeu de 20,000 images publiées par des utilisateurs aléatoires. Ils ont révélé que dans 68% des cas, il était possible d'accéder à une copie de l'image originale, contenant les données relatives à l'originale, comme la position GPS de l'endroit où elle a été prise, et d'autres informations. Ils ont en effet révélé que l'accès aux données relatives aux photos était impossible dans seulement 23% des cas. Cela démontre que l'accès à l'information des utilisateurs est relativement facile. [3]

Ils ont également présenté plusieurs mécanismes de sécurité qu'emploient les grandes entreprises qui pratiquent la collecte de données pour les protéger, mais le problème est que l'implication des utilisateurs est nécessaire. En effet, si les utilisateurs ne gèrent pas bien leurs paramètres de confidentialité, leurs données seront accessibles (nom, lieu d'habitation, de travail, photos…). Par défaut, la majorité des paramètres de confidentialité sont classés « public » ce qui signifie que leur accès est possible par n'importe qui. Les mécanismes de sécurité qu'ils ont présentés révèlent qu'il est impossible d'accéder aux informations d'un utilisateur si celui-ci n'autorise pas cet accès. [4]

La prochaine interrogation à se poser concerne la conscience des utilisateurs. En effet, sont-ils au courant que leurs données peuvent être accessibles publiquement ? Sont-ils consentants du fait que leurs données sont scrutées par les entreprises? Ces interrogations ont été explorées par des chercheurs dans un article intitulé « Impact of User Awareness, Trust, and Privacy Concerns on Sharing Personal Information on Social Media: Facebook, Twitter, and Instagram. », publié en 2018. Ces derniers ont pu conclure que les utilisateurs sont plus enclins à mettre des informations personnelles sur leurs réseaux sociaux quand justement, ils se sentent protégés par les paramètres de confidentialité [5]. Le problème étant qu'ils ignorent ce qui est fait de leurs informations que détiennent les entreprises. La réflexion des utilisateurs se focalise juste sur le fait que leurs informations ne sont pas publiquement par les autres utilisateurs de

la plateforme s'ils ne le souhaitent pas que ce soit le cas, mais ne considèrent pas le fait que les informations sont accessibles par certaines entreprises de vente directe de produits, et donc ne sont pas consentent vis-à-vis de cette situation.

b) Flou normatif

La collecte d'information personnelle que génèrent les gens sur internet est encore quelque chose de relativement nouveau qui est apparu avec l'accroissement d'internet et des technologies de communication. Le sujet n'est pas encadré bien encadré par les lois et présente de nombreuses zones d'ombres à souligner, surtout autour des principes moraux.

Premièrement, dû aux avancées technologiques trop rapides, les gouvernements n'ont pas eu le temps de nécessairement adapter les lois. C'est le point qu'a souligné Kate Mirino, enseignante en droit à l'université de droit de Saint-John. Dans un article sur les lois concernant la collecte des données, elle précise que la croissance rapide qui a eu lieu au cours de ces dernières dizaines d'années a généré des ambiguïtés dans les lois, notamment dans le domaine de la protection des informations. Elle précise que les lois fédérales des États-Unis actuelles ne permettent pas de réguler les pratiques des entreprises. [6]

Par exemple, elle affirme qu'il y'a des clauses dans la constitution fédérale des États-Unis qui parlent de la protection de données personnelles, mais que ces lois s'appliquent aux données personnelles dont la définition anglaise est « informations relating to an identifiable individual », ce qui signifie « informations identifiant un individu ». Or, cette définition est ambiguë et il est difficile de démêler ce qui en fait partie de ce qui ne l'est pas, cela devient donc un véritable jeu d'enfant pour les entreprises de jouer sur cette ambiguïté pour contourner les lois. Elle ajoute aussi que les lois sont obsolètes, car elles ont été établies il y'a au moins de 25 ans, et la situation d'il y a aux 25 ans n'est plus du tout similaire à celle d'actualité. [7]

Elle ajoute que dans certains états [des États-Unis], une liste non exhaustive d'informations à protéger est présente dans leur constitution, celle-ci comprend par exemple l'adresse ou le numéro de téléphone. Finalement, elle affirme que ce type de législation doit être adoptée au niveau fédéral, et pas seulement dans quelques rares états isolés qui ont décidé de faire bouger les choses. [8]

Deuxièmement, le sujet soulève aussi également des dilemmes moraux. En effet, dans un texte scientifique publié par le chercheur et enseignant Andrej Zwitter de l'université de Groningen. Il y'a énormément de problèmes et de flous et dilemmes moraux derrière cette pratique. Il divise sa pensée en

trois catégories d'acteurs : « big data collectors », ceux qui collectent les données, « big data utilizers », ceux qui en font usage et les « big data generators », les acteurs qui génèrent ces informations. Ces acteurs forment un cercle d'interaction, ou les générateurs sont les acteurs les plus importants, mais le problème est que ce cercle d'interaction cause des relations de pouvoir qui ne sont pas balancées. Les agents générateurs ont le moins de pouvoir dans ce cercle alors qu'il s'agit des agents les plus importants, et le cercle d'interactions bénéficie davantage les deux autres parties sans le consentement de l'écrasante majorité des générateurs d'informations [9]. En effet, les entreprises modernes les plus riches sont celles qui exploitent les informations personnelles de leurs utilisateurs aux profits d'autres entreprises, pour des sommes dépassant l'entendement. Par exemple, un rapport de l'université de MIT a révélé que lors de rachat de LinkedIn par Microsoft, ces derniers étaient prêts à payer 260$ par utilisateur actif pour effectuer l'acquisition. [10]

Ensuite, il ajoute que la pratique implique également plusieurs autres dilemmes, par exemple, le fait que ces données soient collectées sur une base journalière crée une virtualisation de la vie de l'individu, et ce, sans qu'il en soit conscient, son passé devient ainsi complètement transparent, contrairement à avant l'avènement de ces pratiques. [11] Le professeur Zwitter affirme que les éthiciens essayent de rester à jour avec les problèmes modernes que pose l'enjeu de la collecte et la gestion des données personnelles, mais que plusieurs livres à la base de leurs réflexions ont été écrits il y a plus de 30 ans, il est donc impossible de déterminer si cette pratique est moralement acceptable selon nos principes actuels. [12]

c) Valeurs en tension

La question de la collecte de données personnelles qu'exercent les multinationales met en jeu de multiples valeurs qu'il est nécessaire de détailler avant de porter une conclusion. Premièrement, comme l'a affirmé le chercheur Andrej Zwitter avec son principe de cercle d'interactions, la collecte de données destinées à la monétisation créée un déséquilibre de pouvoir entre les classes sociales ou un petit sous-groupe est grandement favorisé par cette pratique et profite grandement de la situation, cela implique donc des tensions pour la valeur « richesse » selon la catégorie **pouvoir**. [13]

Un autre souci relatif aux collectes de données concerne le fait que l'analyse de ses données peut permettre l'influence massive des utilisateurs et ainsi, les pousser à la consommation ou encore à effectuer des actions qu'ils n'auraient pas nécessairement effectuées sans cette influence du service qu'ils utilisent. En effet, dans un autre article scientifique publié par l'université de Louisiane, il a été démontré que les publicités affichées par les services qui font de la collecte de données et qui donc

basent les publicités affichées selon les préférences, personnalités, et gout des utilisateurs voient leurs publicités avoir beaucoup moins de chance d'être ignorées par les utilisateurs, et donc l'utilisateur est beaucoup plus enclin à cliquer sur la publicité et à consommer. Cela met en jeu la valeur « pouvoir social » de la catégorie **pouvoir,** car cela permet aux entreprises à la fois de contrôler les achats de milliards d'utilisateurs, mais également d'avoir beaucoup d'influence sur les autres entreprises qui font de la vente directe et qui ont besoin de faire les campagnes de publicité. [14]

Les collections de données impliquent également des valeurs liées à la catégorie « Sécurité », car, selon une recherche effectuée à l'université de Toronto par des chercheurs titulaires de doctorats en pédiatrie et en analyse de données, il a été démontrer que les données collectées par les réseaux sociaux pouvaient être utilisées pour explorer les expériences sociales des adolescents qui souffrent d'un handicap et qui utilisent le service, expériences qu'on a du mal à cerner autrement. L'article révèle en effet que l'extraction de ces données offre un gros avantage à l'analyse du comportement des adolescents et permet d'avoir une bien meilleure compréhension des interactions qu'ils font [15]. Cela fournit en effet des données très utiles à l'analyse de la psychologie des jeunes adultes qui ne sont disponibles nulle part ailleurs. L'analyse de données est utile pour avoir une meilleure compréhension des maladies mentales, notamment des troubles antisociaux chez les adolescents permettant ainsi de développer des soins plus efficaces. Tout cela motiverait la pratique par l'implication la valeur « Santé » de la catégorie **sécurité.**

De plus, les collectes de données permettent aux entreprises de garder leur service qu'ils proposent gratuit et cela permet donc aux utilisateurs de bénéficier du service sans devoir payer. La plupart de ses services auraient été très couteux au vu du fait qu'ils nécessitent énormément d'ingénieurs pour maintenir le tout fonctionnel. Cela met donc en également jeu la valeur « plaisir » appartenant à la catégorie **hédonisme**.

III) Conclusion (position justifiée)

Pour conclure, après avoir raisonné et pensé ma position, il m'est totalement évident de me positionner contre la pratique de collecte de données personnelles destinées à la monétisation qu'effectuent les grandes entreprises.

Bien que comme expliqué précédemment, cela permet aux utilisateurs de bénéficier gratuitement de services considérés comme indispensables à notre époque et que, comme démontré par l'université de

Toronto, l'exploitation des données permettent d'avoir des échantillonnages afin d'effectuer des analyses et ainsi mieux comprendre certains phénomènes psychologiques chez les jeunes [16], ces avantages viennent au détriment d'une régulation inexistante et de principes moraux illégitimes. Premièrement, comme dit à la section « Flou normatif », l'enseignante en droit Kate Mirino à démontrer que cette pratique n'est encore pas assez bien régie par les constitutions des pays ou le phénomène est répandu, il est donc très difficile de tolérer, ou d'être pour la pratique, en sachant que les acteurs n'ont pas de lois spécifique à respecter et peuvent essentiellement agir de la façon qu'ils le désirent [17]. Pour que cela devienne mieux contrôlé, il faudrait donc des lois dénuées de toute ambiguïté et universelles pour toutes les entreprises qui jouent de cette pratique. De cette façon, cela permettrait une bien meilleure régulation et une connaissance plus claire de ce qui est permis, ou pas, d'effectuer à nos informations. Sans de telles lois, ma position demeurera contre la pratique.

En deuxième lieu, bien que selon le rapport « Impact of User Awareness, Trust, and Privacy Concerns on Sharing Personal Information on Social Media: Facebook, Twitter, and Instagram. », semble démontrer que les utilisateurs sont plutôt conscients du fait que leurs informations doivent être classées « privé » pour empêcher l'accès public [18], il manque tout te même leur conscience par rapport au traitement que les entreprises font avec leurs données, pour que la pratique soit acceptable, il faudrait que chaque utilisateur reçoive une alerte lui indiquant le détail sur comment ses données vont être monnayées, autrement c'est difficile d'être pour le fait de laisser la pratique.

IV) Références

[1]: Sardiano, C. Varlamis, I. Bouras, G. (2018) *Extracting user habits from Google maps history logs*. International Conference on Advances in Social Networks Analysis and Mining. p2-8. [en ligne]. repéré à: https://www.researchgate.net/publication/328525395_Extracting_User_Habits_from_Google_Maps_History_Logs

[2]: Facebook, Inc. (2021) *What kinds of information do we collect?* Data Policy. [en ligne]. Repéré à: https://www.facebook.com/policy.php?ref=pf

[3] - [4]: Smith, M. Szongott, C. Henne, B. Voigt, G. (2013) *Big Data Privacy Issues in Public Social Media*. [en ligne]. Repéré à: https://ieeexplore.ieee.org/abstract/document/6227909

[5] – [18]: Paramarta, V. Jiha, M. Dharma, A. Hapsari, I. Puspa, S. Hidaynato, A. (2018) Impact of User *Awareness, Trust, and Privacy Concerns on Sharing Personal Information on social media: Facebook, Twitter, and Instagram.* ICACSIS. p217-276. [En ligne]. Repéré à: https://ieeexplore.ieee.org/document/8618220

[6] – [7] – [8] – [17]: Mirino, K. (2019) *It's Nothing Personal: Why Existing State Laws on Point-of-Sale Consumer Data Collection Should Be Replaced With a Federal Standard.* St. John's Law Review. 93(1), p177-200. [En ligne]
Repéré à: https://scholarship.law.stjohns.edu/lawreview/vol93/iss1/6/

[9] – [11] – [12] - [13] : Zwitter, A. (2014) *Big Data ethics.* Big Data & Society. p1-6. [En ligne] Repéré à: https://journals.sagepub.com/doi/full/10.1177/2053951714559253

[10]: Short, J (2017) *What's Your Data Worth?* MITSloan Management Review. 58(3), p17-19. [En ligne]. Repéré à: https://sloanreview.mit.edu/article/whats-your-data-worth/

[14]: Jung, A. (2017) *The influence of perceived ad relevance on social media advertising: An empirical examination of a mediating role of privacy concern*. Computers in Human Behavior, p303-309. [En ligne]. Repéré à: https://www.sciencedirect.com/science/article/abs/pii/S0747563217300080

[15] – [16]: Walker, M. King, G. Hartman, L. (2018) *Exploring the potential of social media platforms as data collection methods for accessing and understanding experiences of youth with disabilities: a narrative review.* The Journal of Social Media in Society. 7(2), p43-68. [En ligne]. Repéré à: https://thejsms.org/index.php/JSMS/article/view/393