ÉTHIQUE APPLIQUÉE À L'INGÉNIERIE

SSH3501

DE2 : Exploration de la controverse

Groupe 03

Victor Kim

1954607

22 février 2022

Introduction

Mon sujet pour le DE1 était l'automatisation des caisses dans les supermarchés, mais j'ai décidé de changer de sujet et me concentrer sur la collecte des données numériques personnelles des utilisateurs par les entreprises. Ce sujet touche une grande partie de la population moderne aujourd'hui où l'utilisation des appareilles est très commun. Pour optimiser la vente des services, plusieurs compagnies technologiques ont tendance à collecter directement les données des clients pour mieux connaître leurs préférences et leurs besoins dans le but d'améliorer leurs services ou de concevoir des nouveaux produits avec des clients potentiels. Ce concept est connu sous le nom de « Big Data », qui consiste à collecter une quantité énorme de données personnelles, d'analyser ces données et d'utiliser des modèles prédictifs pour deviner les besoins du marché. Cependant, les utilisateurs ne sont pas souvent conscients de la diffusion de leurs données personnelles et des répercussions possibles dans leur vie. Une partie des consommateurs ont plusieurs inquiétudes pour la collecte des données personnelles sans consentement.

La sécurité des données personnelles n'est pas souvent visible par les utilisateurs. Certaines entreprises vont même collecter l'information des utilisateurs vulnérables comme ceux des mineurs qui démontre un manque de responsabilité de la part des professionnels: « *TikTok avait déjà été condamnée en février 2019 à une amende de 5,7 millions de dollars aux États-Unis pour avoir collecté illégalement des données personnelles de mineurs de moins de 13 ans, parmi lesquels leurs noms, adresses courriel et postale.* » (Les affaires, 2021).

Dans cette controverse, il y a deux parties prenantes. Les entreprises et les autorités qui désirent collecter les données d'utilisateurs pour optimiser les ventes de produits et contrôler les utilisateurs et les utilisateurs qui souhaitent protéger leur vie privée en ligne. Dans ce contexte, je vais prendre en considération les incertitudes, le flou normatif et les valeurs en tension pour étudier en profondeur le sujet. Finalement démontrer une position robuste dans cette situation.

Incertitudes

Premièrement, il y a une incertitude sur ce que les entreprises peuvent détenir comme information sur un utilisateur. Avec les limites technologiques, les entreprises peuvent exploiter le fait qu'il n'est pas toujours la possibilité d'avoir le consentement des utilisateurs pour collecter des données personnelles : « *De plus, il est parfois impossible de recueillir le consentement des personnes ou de les informer de façon parfaitement transparente.* » (Rossi, 2018). Les entreprises collectent deux types de données, l'information produite suite à des utilisations par les consommateurs et toutes les actions d'un utilisateur sur un appareil électronique : « *Il est commun de reconnaître que l'utilisation des médias informatisés s'accompagne toujours de la production et du stockage de deux types d'informations : d'une part les informations produites par les utilisateurs (création et partage de contenus, informations personnelles délivrées lors de la création de profils, etc.) et d'autre part les informations résultant d'un enregistrement automatique des actions effectuées par les utilisateurs (temps passé sur un site, contenus consultés, les liens hypertextes actionnés, etc.)* » (Rossi,2018). Toutes sortes d'information dans la vie sociale d'un utilisateur peut être enregistrées dans une base de données d'une entreprise. Les inconnues qui travaillent avec les données de compagnies peuvent facilement accéder aux données personnelles d'un utilisateur dans l'ignorance.

Deuxièmement, il y a une incertitude sur ce qui peut arriver aux données personnelles d'un utilisateur les entreprises. Une nouvelle source de profits pour les entreprises est la divulgation des données personnelles des utilisateurs. L'entreprise peut vendre des données personnelles à d'autres organisations ou partager des données personnelles avec les autorités qui exercent des pressions : « *Il peut arriver que des pressions s'exercent par ailleurs sur les chercheurs pour qu'ils partagent des données de recherche pourtant confidentielles. Ces pressions peuvent venir des services de police ou de renseignement dans certains cas, de l'industrie, mais également d'institutions de recherche incitant au partage et à l'ouverture des données pour favoriser la transparence de la recherche et le partage des connaissances* » (Rossi, 2018). Les données peuvent être vendues à d'autres entreprises qui peuvent avoir des répercussions importantes dans la vie des utilisateurs. Les conséquences peuvent être importantes sur l'image publique dans la société, les accomplissements, la dignité d'un individu : « *Les programmes gouvernementaux de collecte d'informations sont problématiques même lorsque celles-ci ne sont pas transférées à une tierce partie. Ils ne respectent généralement pas les procédures habituelles et sont mis en place à l'insu des personnes concernées. Qui plus est, en rassemblant des données éparses*

d'apparence anodine, le gouvernement peut obtenir des profils et avoir accès à des informations que les personnes souhaitent garder secrètes : état de santé, opinions politiques ou orientation sexuelle… Un tel profilage pourrait renforcer les préjugés ou les discriminations à l'encontre de certains citoyens. » (Maciel-Hibbard, 2018). La divulgation d'information sur la vie privée d'une personne peut facilement influencer son environnement, il peut subir des préjustices par sa famille, ses amis, ses collègues etc.

Flou normatif

Depuis l'expansion de l'utilisation des technologies dans la société, les utilisateurs sont de plus en plus contrôlés et manipulés par les entités qui possède leurs données personnelles : « *Ils exercent ainsi un pouvoir sur les internautes. Il s'agit du pouvoir de surveiller, cibler, analyser, contrôler/manipuler les individus et de façonner leurs comportements* **[…]** *Ce pouvoir est exercé par les capitalistes de surveillance à travers l'architecture ubiquitaire d'appareils et d'objets intelligents interconnectés. Il est essentiel de le comprendre car c'est cette forme de pouvoir qui a réorienté le comportement humain à des fins politiques dans l'affaire* » (Cabas, 2021). Les organisations les plus puissantes ont beaucoup d'influence sur le jugement et les décisions des consommateurs, car ils connaissent très bien les valeurs des individus. Ils peuvent facilement utiliser l'information pour inciter un comportement visé. Cela veut dire qu'une grande majorité des utilisateurs ont déjà l'habitude d'ignorer la collecte des données personnelles, car c'est rendu que tout le monde subit la même chose alors c'est socialement acceptable.

Les organisations gouvernementales comme la FBI et la NSA ne vont pas trop empêcher la collecte des données personnelles des usagers, car ils peuvent également retrouver des avantages dans leur travail d'administration du public. Ils vont donc participer à la surveillance des utilisateurs avec les organisations qui possèdent les technologies nécessaires pour la manipulation de données personnelles : « *Les révélations d'Edward Snowden de 2013 ont confirmé l'accès de la NSA et du FBI aux données des internautes étrangers de Microsoft, Yahoo, Google, Facebook, You Tube et Apple. Outre le programme Prism, d'autres projets ont vu le jour, comme Project Chess (débuté en 2008) de la messagerie Skype pour faciliter l'accès des agences de renseignement américaines aux appels Skype.* **[…]** *Cette accumulation de données, le pouvoir de domination, de manipulation et de contrôle donnent à ces entreprises du numérique un nouveau pouvoir.* » (Cabas, 2021). Les organisations gouvernementales peuvent donc contrôler les entreprises technologiques qui vont à leur tour contrôler les utilisateurs.

Depuis quelques années les politiques pour protéger les données personnelles des utilisateurs ont été amélioré : « *Les cadres juridiques en matière de protection des données se sont étoffés au fil des ans, mais parallèlement s'est développée une législation considérable facilitant les enquêtes et la collecte de renseignements – cette dernière concernant particulièrement les communications sur internet –, renforçant le pouvoir exercé jusque-là de fait par les organismes gouvernementaux. L'équilibre sécurité/vie privée s'est donc dégradé en faveur de la première. Cette évolution a été grandement influencée par la mondialisation du terrorisme et l'entrée du cyberespace dans les problématiques de sécurité.* » (Maciel-Hibbard, 2018). Il y a donc des lois de protection inefficaces pour la protection des données personnelles, car elles n'ont pas vraiment comme but d'empêcher l'identification des usagers, mais plutôt d'améliorer l'administration sociale et la protection internationale du gouvernement en gagnant plus de contrôle sur les citoyens pour optimiser la détection des activités criminelles potentielles.

La morale imposée par la société est que tout le monde a droit d'avoir une vie personnelle où on peut s'exprimer avec liberté et garder des secrets : « *Chacun a droit à la vie, à la liberté et à la sécurité de sa personne; il ne peut être porté atteinte à ce droit qu'en conformité avec les principes de justice fondamentale.* » (Gouvernement du Canada, 2021). Ce qui n'est pas toujours le cas avec les appareils électroniques, car idéalement les usagers vont pouvoir continuer de s'exprimer librement sur les plateformes et de rester anonyme, mais il va toujours avoir des organisations avec des motifs.

Selon l'ordre des ingénieurs du Québec, les valeurs à favoriser dans la profession sont la compétence, le sens de l'éthique, la responsabilité et l'engagement social. Deux valeurs essentielles du côté humain sont le sens de l'éthique et la responsabilité. L'ingénieur doit valoriser le sens de l'éthique est très important, car il faut considérer les conséquences qu'une technologie implantée peut avoir sur les autres. Il faut être honnête et transparent, donc un ingénieur logiciel doit avertir les usagers quand leurs données personnelles sont utilisées.

Valeurs en tension

Dans cette controverse, deux parties prenantes s'opposent. Les entreprises et les autorités qui valorisent le développement économique et le contrôle dans la société. Ils sont en faveur pour la collecte des données personnelles, car c'est une nouvelle ressource qui permet le développement dans plusieurs domaines: « *Les données en elles-mêmes offrent un potentiel extraordinaire que l'on commence à exploiter. Elles permettent de générer des connaissances, qui étaient soit techniquement hors d'atteinte autrefois, soit inexistantes, parce que hors du domaine même du pensable. Une nouvelle médecine se développe, qui, grâce aux données personnelles, sera en mesure de proposer des traitements adaptés à des individus particuliers et non plus seulement calibrés pour des populations. De nouveaux champs scientifiques sont ouverts avec des découvertes réalisables automatiquement sur les masses de données accessibles. Une nouvelle économie émerge, qui exploite les données pour des services à valeur ajoutée. McKinsey [2013] estime le potentiel économique annuel du Big Data pour le système de santé américain à 300 milliards de dollars, soit 1000 dollars par habitant et par an !* » (Frénot, 2014). Les données permettent le partage de connaissances à une échelle mondiale ce qui est essentiel dans plusieurs secteurs de recherches et à l'émergence de nouveaux domaines d'étude. Ces études vont avancer le développement économique. Selon Schwartz, le pouvoir est la différence entre les statuts sociaux, le prestige, l'influence, le contrôle ou la domination des gens. Les entreprises et les autorités défendent donc la richesse et l'autorité de la catégorie du pouvoir. Les consommateurs demandent qu'on respecte leur vie privée et d'avoir la liberté d'expression sans conséquence pendant l'utilisation des appareils électroniques : « *Les attentats du 11 septembre 2001 ont représenté un tournant, et leur impact sur l'opinion a été décisif. En 2002, les Américains se divisaient sur la surveillance par le gouvernement de leurs activités en ligne : 45 % des sondés y étaient favorables, 47 % défavorables.* » (Maciel-Hibbard, 2018). On voit qu'il y a quand même une grande partie de la population américaine qui s'oppose la surveillance par le gouvernement. Selon Schwartz, la maîtrise de sa destinée est l'indépendance de la pensée et d'action, la création, l'exploration. Tout ce qui découle du besoin ou du désir qu'ont les individus d'explorer et de comprendre la réalité en sentant qu'ils ont le contrôle des évènements qui s'y produisent. Une partie des consommateurs défendent donc le respect de soi et la liberté dans la catégorie de la maîtrise de sa destinée.

Conclusion

Pour ma position, je suis contre la collecte des données personnelles sans consentement. Plusieurs entreprises et organismes gouvernementaux justifient que la collecte des données soit importante pour la protection des citoyens ou pour l'amélioration de l'expérience utilisateur qui sont des raisons valides. Cependant, je suis convaincu que la protection des citoyens est souvent juste utilisée comme prétexte pour mieux surveiller et contrôler les citoyens selon des visions politiques. Les crimes internationaux comme les activités terrorismes ne sont pas des situations qui arrivent tous les jours. De plus, il existe d'autres façons d'améliorer l'expérience utilisateur pour les produits. Les compagnies peuvent toujours créer des sondages ou des forums pour la discussion sur les améliorations possibles d'un produit, mais ils sont plus intéressés à conserver et manipuler les données personnelles comme l'état de santé, les opinions politiques et l'orientation sexuelle mentionnée par Marilia Maciel-Hibbard une doctorante en science de l'information et de la communication. En considérant les incertitudes, le flou normatif, les valeurs en tension et en tant qu'étudiant en ingénierie, je suis fort convaincu que la collecte des données personnelles sans consentement manque de transparence et de responsabilité.

Bibliographie principale :

[1] Rossi, J. Biggot, J-E. (2018). Traces numériques et recherche scientifique au prisme du droit des données personnelles. [en ligne]. https://www.cairn.info/revue-les-enjeux-de-l-information-et-de-la-communication-2018-2-page-161.htm

[2] Maciel-Hibbard, M. (2018). Protection des données personnelles et cyber(in)sécurité. [en ligne]. https://www.cairn.info/revue-politique-etrangere-2018-2-page-55.htm

[3] Cabas, R. (2021). Le pouvoir instrumentarien et le Big Data à l'ère de la domination numérique. [en ligne]. http://mai68.org/spip2/IMG/pdf/Big-data_Pouvoir-instrumentarien_sept2021.pdf

[4] Frénot, S. Grumbach, S. (2014). Les données sociales, objets de toutes les convoitises. [en ligne]. https://www.cairn.info/revue-herodote-2014-1-page-43.htm

Bibliographie complémentaire :

[5] Les affaire. (2021). TikTok poursuivi pour collecte de données personnelles d'enfants. [en ligne]. https://www.lesaffaires.com/techno/internet/tiktok-poursuivi-pour-collecte-de-donnees-personnelles-d-enfants/624425

[6] Gouvernement du Canada. (2021). Article 7 – Droit à la vie, à la liberté et la sécurité de la personne. [en ligne]. https://www.justice.gc.ca/fra/sjc-csj/dlc-rfc/ccdl-ccrf/check/art7.html