

**ÉTHIQUE APPLIQUEÉ À L'INGÉNIERIE**

**SSH3501**

**DE3 : Synthèse critique et personnelle**

**Victor Kim**

**1954607**

**12 avril 2022**

**Rappel du sujet**

Pour le DE2, mon sujet était sur la collecte des données numériques personnelles des utilisateurs sans consentement par les entreprises et les autorités gouvernementales qui est un problème contemporain concernant plusieurs dans la société. Pour l’optimisation des profits, les compagnies doivent bien connaître les préférences des clients. Ils vont avoir un meilleur contrôle sur l’orientation du produit et les clients. Plus qu’ils répondent aux besoins des clients, plus les clients vont être loyaux envers la compagnie. Quand un produit répond à des besoins spécifiques, la compagnie peut gagner des nouveaux clients.

Pour obtenir ces ressources d’information, il existe plusieurs méthodes. En utilisant les « cookies » des fichiers locaux qui permettent l’enregistrement des sites visités et des actions effectués. Un système utilise ces fichiers pour proposer des publicités personnalisées. L’historique sauvegardé dans les navigateurs est un autre moyen pour collecter des données personnelles. Un moyen moins direct est d’acheter les données numériques d’une autre compagnie. **[1]**

La sécurité des données personnelles est souvent remise en question. Dans la controverse, une partie prenante est composée des utilisateurs qui souhaitent pouvoir conserver leur identité et vie privée quotidienne. L’autre partie prenante est composée des compagnies et les autorités gouvernementales qui désirent optimiser la vente de leur produit et augmenter leur contrôler sur les utilisateurs en utilisant la surveillance.

**Les valeurs en tension**

La valeur défendue par une partie des utilisateurs est la maîtrise de sa destinée qui est selon Schwartz, l’indépendance de la pensée et d’action où un individu a le contrôle de ses propres actions et à la liberté sur sa réflexion et ses opinions. L’individu a le droit d’explorer lui-même. La seconde valeur en tension est le pouvoir qui est défendu par la partie prenante composée des compagnies ou un organisme avec un certain pouvoir social. Le pouvoir selon Schwartz est la différence entre les statuts sociaux où une personne ou un groupe est considéré supérieur aux autres dans la société, le prestige. Avoir du pouvoir c’est exercer une influence, un contrôle sur les autres et être capable de les dominer.

**Analyse de la situation**

L’éthique de responsabilité se divise en deux formes. La première qui est un devoir où il existe une liste de responsabilités bien définie qu’un individu doit s’assurer de respecter. La deuxième repose plus sur les sentiments de l’individu. C’est le cas où un individu se sent responsable de faire quelque chose. La responsabilité en éthique donne l’obligation à un individu de sortir de sa zone de confort et le force à faire ses propres réflexions.

Selon la définition de Max Weber, un individu est responsable de trois choses. Ses intentions, ses compétences et des conséquences prévisibles. Par exemple, un groupe de spécialistes l’Electronic Frontier Foundation lance des pétitions contre les applications « stalkerware » qui sont faites pour surveiller les appareils électroniques. Les membres de l’organisation ont l’intention d’aider les gens à protéger leur information personnelle. Ils doivent aussi considérer qu’à la suite de l’élimination des applications de surveillance, les victimes de la violence domestique vont avoir moins de protection dans plusieurs situations. **[2]**

Pour la partie devoir de l’éthique de responsabilité, la loi sur la protection des renseignements personnels dans le secteur privé indique qu’il faut seulement collecter les données personnelles nécessaires quand ça concerne un intérêt sérieux et légitime. Par exemple, les ingénieurs logiciels qui travaillent pour l’autorité gouvernementale doivent s’assurer de bien respecter les normes demandées. Les programmes construits vont devoir avoir les restrictions nécessaires pour empêcher qu’un policier ne soit pas capable de facilement accéder à l’information personnelle des suspects durant les enquêtes. L’individu a l’obligation d’agir parce qu’une autorité l’oblige. **[3]**

L’idée de l’éthique prospective est qu’il faut bien penser aux conséquences que l’acte d’un individu peut avoir sur les autres. Il faut avoir un sentiment d’urgence et être responsable des conséquences d’un acte. Selon Hans Jonas, il faut avoir une responsabilité envers les autres qui sont plus vulnérables. Par exemple, en tant que professionnel dans le domaine technologique, un ingénieur logiciel a la responsabilité envers les utilisateurs des produits électroniques qui sont plus vulnérables, car ils sont moins informés sur comment protéger leur information personnelle.

La première action nécessaire qu’un individu doit prendre pour prévenir les conséquences est qu’il doit imaginer les effets possibles liés à une action. Par exemple, le développement d’une fonctionnalité de création d’un compte va en quelque sorte toucher à l’identité personnelle d’un utilisateur. Il faut donc savoir qu’il est possible que l’information soit divulguée ou volée. La deuxième action nécessaire est qu’un individu doit craindre les conséquences de ses actions, il doit être sensible et être conscient qu’on est ignorant des menaces et dangers possibles. Par exemple, un ingénieur logiciel doit craindre qu’à la suite de la collecte de données personnelles d’une personne, s’il y a diffusion de certaines informations, sa vie sociale peut être endommagée. L’entourage de l’individu peut commencer à avoir des préjugés sur lui. Il peut avoir de la difficulté à se trouver un emploi.

Pour la partie sentiment de l’éthique de responsabilité, c’est plus un individu qui a sa propre réflexion sur la situation dont il fait face et il décide d’agir selon sa réflexion. Par exemple, Edward Snowdon qui travaillait pour l’Agence nationale de sécurité a remarqué que le programme de surveillance internationale violait plusieurs droits humains. Les conversations privées, les messages étaient sauvegardés. La vie des gens était filmée et enregistrée dans des bases de données. Les citoyens n’avaient plus de vie privée, ils étaient constamment surveillés. Snowdon a fait ses propres réflexions et il a décidé d’exposer les secrets du gouvernement était la bonne chose à faire. **[4]**

Le concept indique qu’il est impossible de reconnaître toutes les conséquences de nos actions. L’ingénieur a la responsabilité de penser à l’avenir qu’il ne connaît pas et se sentir engagé. Il doit savoir que ses actions peuvent causer des conséquences incontrôlables et s’assurer de mettre en place des mesures pour gérer des risques. Ces risques sont identifiés seulement à partir des connaissances incomplètes. Il doit s’assurer de ne pas mettre les générations futures en péril. Par exemple, les ingénieurs logiciels qui travaillent dans des entreprises qui pratiquent la collecte de données personnelles doivent s’assurer de prendre des mesures de précaution pour introduire l’anonymisation des données. Ils doivent considérer qu’il est possible qu’il ait des groupes d’utilisateurs plus vulnérables comme des mineurs. **[5]**

L’éthique de discussion selon Habermas vise le questionnement et la circulation de l’information. Les trois premières règles expliquent sur comment les gens doivent se comporter durant les discussions. L’individu doit exprimer ses idées aux autres et en même temps écouter les idées des autres. Il ne doit pas juste laisser les autres parler et ne rien dire et il ne doit pas empêcher les autres à s’exprimer. L’individu ne doit pas essayer d’utiliser les autres comme des moyens pour accomplir leur objectif. L’individu ne doit pas essayer de cacher la vérité ou accepter que les autres soient en train de mentir. Un utilisateur ne doit pas complètement rejeter l’idée de la collecte de données personnelles. Il doit commencer par comprendre pourquoi les compagnies implémentent ces programmes. Il est possible que la collecte de données ait des impacts positifs par exemple, l’utilisateur peut avoir une meilleure expérience pendant la consommation d’un produit ou si une personne est en danger, on peut facilement localiser la personne et envoyer de l’aide. Les dirigeants de Facebook ne doivent pas demander aux employés de vendre des données personnelles à une autre compagnie juste pour augmenter ses profits. De plus, les employés de Facebook ne doivent pas mentir aux usagers que la compagnie vend des données personnelles. **[6]**

La quatrième règle essaie de mettre en place une harmonisation de deux concepts. L’universalisation kantien qui demande à l’individu de ne pas juste considéré ses propres intérêts. Il ne faut pas se faire contrôler par ses préférences, il faut faire ce qu’un être humain doit faire pour le bien des autres. Dans cette règle, il faut considérer que tout le monde est égal. L’autre concept est le bien commun de Bentham et Mill où il faut bien comprendre l’idée des autres avant de trouver une décision qui serait bonne pour tout le monde donc les conséquences vont déterminer l’action est considérée éthique ou non. Il faut savoir qu’en ayant plus de points de vue, on peut prendre sélectionner les avantages de chacun pour créer une idée avec plus d’avantages. Il existe des solutions où les compagnies et les clients sont satisfaits. « ShareWell » une compagnie qui vend des applications d’enregistrement d’écran laisse les clients donner leurs opinions sur l’utilisation du produit. Dans ce cas, la compagnie peut travailler avec des vraies données pour l’amélioration de leur produit et les clients peuvent protéger leurs données personnelles. **[7]** Les dirigeants de la compagnie ne sont pas en train de juste penser aux profits qu’ils peuvent ramener, ils considèrent leurs clients en tant qu’être humain égal avec les mêmes droits et libertés et que les clients cherchent à conserver leur intimité.

Les trois dernières règles reposent sur l’acceptabilité sociale où on cherche à trouver un consensus. Donc une décision où tout le monde est satisfait dans une discussion et on n’arrive pas à un consensus, il faut trouver la source du conflit. Donc la partie qui amène des personnes à ne pas être en accord avec la décision et par la suite, chercher un compromis éthique. Chaque partie va devoir céder quelque chose dans la décision finale. Il faut assurer la présence de l’acceptabilité sociale, tout le monde qui participe à la discussion à doit être entendu. Par exemple, une compagnie qui a absolument besoin de données utilisateurs pour améliorer leur produit et que les utilisateurs refusent de laisser la compagnie sauvegarder leurs données. Les deux parties prenantes peuvent discuter ensemble pour essayer de se trouver un consensus. La compagnie peut essayer de proposer des méthodes de protection pour masquer l’identité pendant l’extraction de données. Si les utilisateurs laissent la compagnie collecter leurs données et que la compagnie accepte d’offrir assez de protection pour les utilisateurs et masquer leurs identités, donc ils vont trouver un consensus ensemble. La décision prise est définie par les normes de protection données et par les procédures à suivre pour la récolte des données utilisateurs. On prend en compte l’opinion des gens qui sont affectés par la collecte des données personnelles et on porte attention à leurs jugements sur la décision.

L’impartialité des normes va dépendre de l’objectivité des résultats. Donc plus les résultats ne donnent pas d’avantages à un groupe particulier de personne plus les normes associées sont impartiales. Dans la discussion, on veut que les résultats soient le plus universel possible, donc avoir le plus de monde en accord possible pour faciliter l’acceptabilité d’un compromis. L’idée est que le bien du groupe est plus important que le bien d’un seul individu.

**Conclusion**

Après cette réflexion, je suis convaincu que je suis contre la collecte de données utilisateurs sans consentement. L’éthique de responsabilité a permis de montrer qu’il faut être responsable de ses intentions, de ses compétences et des conséquences qu’on peut prévoir de nos actions. Donc l’individu a le devoir de répondre à des attentes que les autres lui imposent. Ceci s’applique à la partie prenante composée de certains employés professionnels qui travaillent dans les compagnies informatiques qui pratiquent la collecte des données utilisateurs. Ils doivent être responsables de protéger les données de ses utilisateurs. Dans plusieurs cas, c’est une demande plus idéaliste les données personnelles ne sont pas protégés parfaitement. En utilisant les trois premières règles de l’éthique de discussion de Habermas qui demande à tous les individus dans une discussion d’être bienveillant, de ne pas manipuler les autres et de ne pas raconter des mensonges. On sait qu’en pratique il serait peu probable. Il va toujours avoir des individus qui vont vouloir tirer plus d’avantages quand l’opportunité se présente. Un bon exemple est qu’en 2020, Facebook s’est fait poursuivre en cours pour avoir collecté des données utilisateurs sans consentement et a échangé ces données sous le prétexte de pouvoir mieux cibler des idées économiques. **[8]**

L’éthique de prospective implique qu’il faut penser aux conséquences que nos actions peuvent avoir sur les autres. Donc un individu a le devoir de s’occuper des autres qui sont plus vulnérables que lui. Il doit être conscient qu’il ne peut pas connaître toutes les conséquences liées à ses actions et qu’il doit craindre de produire des résultats irréversibles. Mon argument principal est que même si les personnes qui ont accès aux données privées des utilisateurs sont bienveillants et protègent de leur mieux les utilisateurs, ils n’ont aucun contrôle sur les sources des conséquences imprévisibles. En 2015, une cyber attaque sur Ashley Madison a propagé l’information de plusieurs utilisateurs. Ces données ont causé plusieurs divorces dans les familles et ont contribué à l’augmentation du taux de suicide. **[9]** Personnellement, je pense que tant qu’on fait confiance aux autres et qu’on leur donne accès à quelque chose d’important, il va toujours avoir des risques présents. Donc interdire la collecte de données personnelles sans consentement par les compagnies et les autorités gouvernementales va diminuer exponentiellement les conséquences.

**Références**

**Du DE1 :**

Sujet changé à partir du DE2

**Du DE2 :**

**[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

**[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

**Du DE3 :**

**[1]** Pastore, C. (2019). Ce qu’il faut savoir sur la collecte de nos données personnelles. [En ligne] : <https://mbamci.com/donnees-personnelles-ce-quil-faut-savoir/>

**[2]** Radio-Canada. (2019). Une coalition contre les applications d’espionnage de partenaire voit le jour. [en ligne] <https://ici.radio-canada.ca/nouvelle/1400244/coalition-contre-against-stalkerware-espion-espionnage-partenaire-conjoint-conjointe>

**[3]** Conseil de l’Europe. (2018). Guide pratique sur l’utilisation de données à caractère personnel dans le secteur de la police, p.4. [en ligne] <https://rm.coe.int/t-pd-201-01-guide-pratique-sur-lutilisation-de-donnees-a-caractere-per/16807927d6>

**[4]** Deléage, J-P. (2014). Un monde sous surveillance totale. [en ligne] <https://www.cairn.info/revue-ecologie-et-politique1-2014-1-page-5.htm>

**[5]** Renforcer la protection de la vie privée dans l’ère numérique. [en ligne]<https://www.ic.gc.ca/eic/site/062.nsf/fra/h_00107.html>

**[6]** Dor, F. (2020). Vendre ses données personnelles : Une business controverse. [en ligne] <https://start.lesechos.fr/societe/culture-tendances/vendre-ses-donnees-personnelles-un-business-controverse-1273442>

**[7]** Kreisberg, S. (2020). Importance of Customer Feedback in software Development. [en ligne] <https://sharewell.eu/why-customer-feedback-is-important-when-it-comes-to-software-development/>

**[8]** TechRepublic Staff. (2020). Facebook data privacy scandal: A cheat sheet. [en ligne] <https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/>

**[9]** Doffman, Z. (2019). Ashley Madison Has Signed 30 Million Cheating Spouses. Again. Has Anything Changed? [en ligne] <https://www.forbes.com/sites/zakdoffman/2019/08/23/ashley-madison-is-back-with-30-million-cheating-spouses-signed-since-the-hack/?sh=4090c5923878>