Lex Electronica

Lex Electronica

Protection de la vie privée dans le contexte des plateformes en ligne : les limites des fiducies de données et du devoir fiduciaire de loyauté

Michelle Albert-Rochette, Clara Lavis et Mathilde Meunier

Volume 28, numéro 1, 2023

URI : https://id.erudit.org/iderudit/1108621ar
DOI : https://doi.org/10.7202/1108621ar

Aller au sommaire du numéro

Éditeur(s)

Centre de recherche en droit public Université de Montréal

ISSN

1480-1787 (numérique)

Découvrir la revue

Citer cet article

Albert-Rochette, M., Lavis, C. & Meunier, M. (2023). Protection de la vie privée dans le contexte des plateformes en ligne : les limites des fiducies de données et du devoir fiduciaire de loyauté. *Lex Electronica*, *28*(1), 23–59. https://doi.org/10.7202/1108621ar

Résumé de l'article

Les lois de protection des renseignements personnels se sont traditionnellement ancrées dans une perspective individualiste de la vie privée dont la pierre angulaire est le mécanisme du consentement individuel. Face aux géants du web, dont le modèle d'affaires repose sur l'analyse de données personnelles, cette perspective paraît inadaptée : elle tient insuffisamment compte des asymétries de pouvoir et d'information en présence et suppose à tort la vie privée comme une question de nature individuelle en omettant ses implications collectives. Elle peine ainsi à protéger adéquatement les personnes et facilite de ce fait la survenance d'effets individuels et sociétaux préjudiciables. Cet article rappelle d'abord les principales limites de la conception individualiste de protection de la vie privée – le modèle du *notice and choice*, ou *notice and consent* – au regard des pratiques des plateformes en ligne. Sont ensuite envisagées, dans une perspective critique, deux pistes de solution juridiques issues d'une conception collective de la vie privée : les fiducies de données et leur appréhension par le droit commun québécois, suivies des obligations fiduciaires de *common law*, et plus particulièrement le devoir fiduciaire de loyauté. Si ces pistes de solution semblent prometteuses à plusieurs égards, elles présentent toutes deux des limites importantes qui rendent difficilement concevable leur implémentation. D'une part, les fiducies de données, reposant sur le choix individuel de confier ses renseignements personnels à un acteur externe, reproduisent les difficultés liées au mécanisme de consentement individuel du modèle classique de *notice and choice*. Leur mise en oeuvre effective requiert également l'intérêt, la compréhension et la confiance des personnes dans le mécanisme, des garanties loin d'être acquises. D'autre part, l'imposition d'un devoir de loyauté obligerait les plateformes à modifier en profondeur leurs pratiques commerciales actuelles, des changements qui ne s'imposeraient pas sans résistance. Le droit à la vie privée, tant dans sa conception individuelle que collective, ne suffit pas à protéger adéquatement les personnes dans l'environnement numérique. D'autres domaines de régulation doivent être appelés à intervenir.

PROTECTION DE LA VIE PRIVÉE DANS LE CONTEXTE DES PLATEFORMES EN LIGNE : LES LIMITES DES FIDUCIES DE DONNÉES ET DU DEVOIR FIDUCIAIRE DE LOYAUTÉ

Michelle Albert-Rochette[1], Clara Lavis[2] & Mathilde Meunier[3]

1 Candidate à la maîtrise en droit avec mémoire à l'Université Laval, Québec

2 Avocate stagiaire, Barreau de Dinant, Belgique

3 Juriste, Paris

Table des matières

RÉSUMÉ

Les lois de protection des renseignements personnels se sont traditionnellement ancrées dans une perspective individualiste de la vie privée dont la pierre angulaire est le mécanisme du consentement individuel. Face aux géants du web, dont le modèle d'affaires repose sur l'analyse de données personnelles, cette perspective paraît inadaptée : elle tient insuffisamment compte des asymétries de pouvoir et d'information en présence et suppose à tort la vie privée comme une question de nature individuelle en omettant ses implications collectives. Elle peine ainsi à protéger adéquatement les personnes et facilite de ce fait la survenance d'effets individuels et sociétaux préjudiciables. Cet article rappelle d'abord les principales limites de la conception individualiste de protection de la vie privée – le modèle du *notice and choice*, ou *notice and consent* – au regard des pratiques des plateformes en ligne. Sont ensuite envisagées, dans une perspective critique, deux pistes de solution juridiques issues d'une conception collective de la vie privée : les fiducies de données et leur appréhension par le droit commun québécois, suivies des obligations fiduciaires de *common law*, et plus particulièrement le devoir fiduciaire de loyauté. Si ces pistes de solution semblent prometteuses à plusieurs égards, elles présentent toutes deux des limites importantes qui rendent difficilement concevable leur implémentation. D'une part, les fiducies de données, reposant sur le choix individuel de confier ses renseignements personnels à un acteur externe, reproduisent les difficultés liées au mécanisme de consentement individuel du modèle classique de *notice and choice*. Leur mise en œuvre effective requiert également l'intérêt, la compréhension et la confiance des personnes dans le mécanisme, des garanties loin d'être acquises. D'autre part, l'imposition d'un devoir de loyauté obligerait les plateformes à modifier en profondeur leurs pratiques commerciales actuelles, des changements qui ne s'imposeraient pas sans résistance. Le droit à la vie privée, tant dans sa conception individuelle que collective, ne suffit pas à protéger adéquatement les personnes dans l'environnement numérique. D'autres domaines de régulation doivent être appelés à intervenir.

Mots-clés : vie privée, données personnelles, fiducies (*trusts*), plateformes, devoir de loyauté

ABSTRACT

Privacy laws have traditionally been rooted in an individualistic perspective of privacy based on the mechanism of individual consent. When considering the practices of the web giants, whose business model is based on the exploitation of personal data, this perspective seems inadequate: it takes insufficient account of the asymmetries of power and information involved and wrongly assumes that privacy is an individual matter. It therefore fails to adequately protect individuals and thus facilitates the occurence of harmful effects. We first recall the limits of the individualistic conception of privacy protection – the notice and choice or notice and consent model – in relation to the online platforms practices. We then critically consider two solutions based on a collective conception of privacy: data trusts and their apprehension by Quebec civil law, followed by canadian common law fiduciary duties, and more particularly the fiduciary duty of loyalty. While these approaches seem promising, they both have significant limitations that make their implementation difficult to conceive. Firstly, data trusts, based on individual choice to entrust one's data to an external actor, replicate the difficulties associated with the notice and choice model. Their effective implementation also presupposes the interest, understanding and trust of individuals in the mechanism, which are far from being acquired. Secondly, the imposition of a duty of loyalty would require platforms to dramatically change their current business practices, changes that would not come without resistance. Privacy law, both in its individual and collective conception, is insufficient to adequately protect individuals in the digital environment. Other areas of regulation must be brought into play.

Keywords: privacy law (online privacy), personal data, trusts, platforms, duty of loyalty

INTRODUCTION

[1] Le modèle d'affaires des plateformes en ligne[4] repose sur la collecte et le traitement des données personnelles (GROUPE D'EXAMEN[5], 2020, p. 210). Sur *Facebook*, par exemple, les « j'aime », la localisation, les transactions en magasin, l'activité des personnes sur d'autres sites web et les comptes avec lesquels elles interagissent[6] sont autant de données rassemblées et croisées entre elles pour permettre l'émergence d'un nouveau savoir ayant une valeur particulièrement intéressante pour les publicitaires (GRAEF, 2016, p. 1). En effet, l'analyse de ces données permet de répartir les internautes en différents groupes algorithmiques (DÉZIEL, 2018, p. 838-839 ; DU PERRON, 2020, p. 37), ou profils types, de façon à leur afficher des publicités *a priori* pertinentes. Il n'y a pas de vente de données personnelles aux entreprises. Il s'agit plutôt de la vente d'un service de ciblage du public visé par les publicitaires. Les intérêts et préférences des internautes deviennent ainsi des produits commercialisables par le biais des audiences ciblées (GRAEF, 2016, p. 1 ; VÉLIZ, 2022, p. 49). Ces techniques de profilage sont en principe acceptées par les internautes au moment de leur inscription. Cependant, peut-on parler de consentement libre et éclairé lorsque tout pousse à se soumettre aux conditions d'utilisation ? Les personnes ne disposent souvent pas des connaissances nécessaires pour comprendre ce à quoi elles consentent, la négociation n'est pas possible et la domination du marché par une poignée d'acteurs remet en question la capacité même de choix (RICHARDS & HARTZOG, 2019, p. 1478-1479 et 1487-1488 ; ALLEN, 2016, p. 72 ; LAZARO & LE MÉTAYER, 2015, p. 796 et 803). Une fois leur inscription complétée, les personnes sont par ailleurs soumises à des techniques comportementalistes, comme le *nudging* (THALER & SUNSTEIN, 2008), qui les poussent à agir dans le sens souhaité par les plateformes (RICHARDS & HARTZOG, 2021, p. 973-975). Et si cette atteinte à l'autonomie se répercute au niveau individuel, notamment sur les habitudes d'achat, elle est aussi à même d'entraîner des conséquences sociétales préjudiciables. Le scandale de *Cambridge Analytica*, où les données de millions d'utilisateurs et d'utilisatrices de *Facebook* ont été utilisées à des fins de profilage politique en vue d'influencer le résultat d'élections (DETROW, 2018 ; GONZÁLEZ, 2017 ; VÉLIZ, 2019), en est un exemple. Face aux pratiques des plateformes en ligne, l'encadrement juridique classique des renseignements personnels n'est plus adapté. Si pendant longtemps le législateur s'est abstenu d'intervenir de peur de freiner l'innovation technologique (BENYEKHLEF, 2018, p. 295-296), il semble désormais urgent de combler les lacunes juridiques pour contrer l'asymétrie de pouvoir entre les plateformes et les internautes, et la survenance d'effets préjudiciables y étant associée.

[2] Dans un premier temps, nous rappelons les principales limites de l'approche dominante en matière de protection de la vie privée, qui conçoit cette dernière au travers du prisme de l'individualisme. Nous faisons ensuite l'examen critique de deux pistes de solution juridiques issues d'une conception collective de la vie privée. Nous

4 Aux fins du présent article, les termes « plateformes en ligne » ou « plateformes » font référence aux grands intermédiaires numériques : « intermediaries that have tremendous power in the marketplace in their role mediating between third parties and connecting users/buyers with producers/sellers » (Laidlaw, 2021, p. 7). Bien que les plateformes en ligne puissent être distinguées selon plusieurs aspects, nous insistons ici sur une de leurs caractéristiques communes : leur pouvoir de marché issu de l'exploitation de données personnelles (Birch et al, 2021, p. 2).

5 Groupe d'examen du cadre législatif en matière de radiodiffusion et de télécommunications, Canada.

6 Meta, À propos des publicités Facebook, 2022, en ligne : <https://www.facebook.com/ads/about/?entry_ product=ad_preferences_hub>.

nous penchons d'abord sur les fiducies de données et sur leur appréhension potentielle par le droit commun québécois (HULIN, 2020 ; LEBLANC, 2020 ; LEBLANC, 2021). En nous appuyant notamment sur une proposition de GUEVARA (2021), nous abordons ensuite les obligations fiduciaires de *common law* pouvant naître indépendamment de la constitution d'une fiducie, et traitons plus particulièrement du devoir fiduciaire de loyauté[7]. Les limites et solutions examinées dans cet article sont analysées au regard des pratiques des plateformes en ligne.

1. D'UNE APPROCHE INDIVIDUALISTE À UNE APPROCHE COLLECTIVE

[3] Traditionnellement, la vie privée s'appuie sur des notions de dignité personnelle et d'intégrité. Des notions purement individualistes qui, à l'ère d'Internet, comportent des questions relatives à l'identité des personnes et à la façon dont leurs renseignements personnels sont traités (LECHEVALIER, 2020, p. 2). Nous revoyons ici la théorie individualiste du contrôle, qui connaît quelques difficultés à l'ère de l'hyperconnexion du monde, au profit d'une théorie collective de la vie privée.

1.1. LA THÉORIE INDIVIDUALISTE DU CONTRÔLE ET LE MODÈLE DE *NOTICE AND CHOICE*

[4] La théorie dominante en matière de protection de la vie privée est celle du contrôle (FAIRFIELD & ENGEL, 2015, p. 408), qui vient s'intéresser particulièrement à la vie privée informationnelle[8], c'est-à-dire aux renseignements personnels. Cette théorie conçoit la vie privée comme relevant du contrôle qu'une personne est en mesure d'exercer sur les modalités de circulation et de diffusion de ses informations personnelles (BENYEKHLEF & DÉZIEL, 2018, p. 28 ; GAUTRAIS & TRUDEL, 2010, p. 59-60, 66-73 ; WESTIN, 1967, p. 7) et entretient ainsi un lien étroit avec les notions d'autonomie, de dignité et de liberté individuelles (BENYEKHLEF & DÉZIEL, 2018, p. 26-27). Dans les lois de protection des renseignements personnels, le contrôle est opérationnalisé au moyen du mécanisme de consentement individuel. Au Québec, la Loi sur les renseignements personnels dans le secteur privé[9] (ci-après « Loi sur le privé ») prévoit par exemple que le consentement pour la collecte, l'utilisation ou la communication d'un renseignement personnel doit être « manifeste, libre, éclairé et […] donné à des fins spécifiques[10]. Le consentement constitue aussi le fondement de la LPRPDE[11] (CPVP[12], 2016), qui l'avait d'ailleurs érigé à son Annexe 1 comme principe obligatoire[13] de traitement de l'information devant être respecté par les organisations,

7 Pour un aperçu d'autres modes de gestion collective des données non examinés dans cet article : Mozilla Insights, J. van Geuns et A. Brandusescu, Shifting Power Through Data Governance, 2020, en ligne : <https://assets.mofoprod.net/network/documents/ShiftingPower.pdf>.

8 Sur les différentes déclinaisons de la notion de vie privée en fonction de son domaine d'application (vie privée territoriale, personnelle et informationnelle) : *R.* c. *Dyment*, (1988) 2 R.C.S. 417, par. 19-22.

9 Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ, c. P-39.1 (ci-après « Loi sur le privé »).

10 *Id.*, article 14 alinéa 1.

11 Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, c. 5 (ci-après « LPRPDE »).

12 Commissariat à la protection de la vie privée du Canada.

13 Par. 5(1) LPRPDE.

sous réserve de certaines exceptions. Plus récemment, le projet de loi 64, adopté par le Parlement québécois en septembre 2021[14], et le projet de loi fédéral C-27[15], ont tous deux cherché à renforcer le consentement en ajoutant des exigences supplémentaires à son obtention par les organisations dans certaines situations[16]. Les lois canadienne et québécoise de protection des renseignements personnels dans le secteur privé adhèrent ainsi au paradigme individualiste, ou personnaliste (DÉZIEL, BENYEKHLEF & GAUMOND, 2020, p. 21) de la vie privée, consolidant un régime de *notice and choice* où les entités doivent de manière générale informer les personnes et obtenir leur autorisation avant de collecter et d'utiliser leurs renseignements personnels (WARNER, 2020, p. 173-174).

[5] Le consentement est donc la base même de la relation que nous avons avec de nombreux sites et entreprises sur Internet, et notamment avec les plateformes en ligne (RICHARDS & HARTZOG, 2019, p. 1461). Par la création d'un compte sur une plateforme, les internautes consentent que cette dernière collecte et utilise leurs renseignements personnels. Un rapport du CPVP avait d'ailleurs mis de l'avant que le réseau social *Facebook* étant gratuit, ses utilisateurs et utilisatrices devaient être disposés à recevoir certaines formes de publicité, essentielle à la fourniture du service, et nécessitant l'utilisation de certains de leurs renseignements personnels (DENHAM, 2009, par. 134).

1.2. LES ÉCHECS DU MODÈLE DE *NOTICE AND CHOICE* FACE AUX PRATIQUES DES PLATEFORMES EN LIGNE

[6] À l'ère de la « mise en données du monde », la théorie individualiste du contrôle rencontre plusieurs limites et permet à certains acteurs d'utiliser ces renseignements dans leurs propres intérêts (DE SAINT PULGENT, 2016, p. 4). Le principal échec de cette conception de la vie privée n'est autre que le modèle du *notice and choice*, ou *notice and consent*, et précisément le consentement en lui-même. En effet, les législations actuelles se confrontent à quelques lacunes face aux pratiques des plateformes en ligne.

1.2.1. UNE COLLECTE DE DONNÉES À L'INSU DES PERSONNES

[7] Les données personnelles des internautes peuvent être collectées par les plateformes à leur insu et sans leur consentement. S'appuyant notamment sur le rapport du professeur Douglas C. Schmidt (SCHMIDT, 2018), c'est d'ailleurs à cette

14 Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, projet de loi nO 64, L.Q. 2021, c. 25.

15 Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois, projet de loi nO C-27 (dépôt et 1re lecture – 16 juin 2022), 1re sess., 44e légis. (Can.).

16 À son article 110, le projet de loi 64 modifie par exemple l'article 14 al. 1 de la Loi sur le privé en prévoyant notamment que le consentement soit « demandé [pour] chacune [des] fins en termes simples et clairs » et que la personne qui le donne puisse obtenir de l'assistance « afin de l'aider à comprendre la portée du consentement demandé ». De son côté, le projet de loi fédéral C-27 prévoit à son paragraphe 15(4) que les renseignements requis pour l'obtention du consentement soient communiqués par les organisations dans « un langage clair et raisonnablement compréhensible ». Le projet de loi C-27 prévoit aussi à son paragraphe 15(6) le principe de consentement explicite pour les « activités d'affaires », à moins d'entrer dans les exceptions du paragraphe 18(3). Les projets de loi 64 et C-27 facilitent toutefois la collecte et le traitement des données personnelles dans d'autres situations, dans une perspective de valorisation des données à des fins d'innovation. À ce sujet, voir : P.-L. Déziel, « La valorisation des renseignements personnels au Québec et au Canada : la promesse des projets de loi no 64 et C-11 », 2021, Les Cahiers de propriété intellectuelle, V33, N2, p. 1193-1240; Borden Ladner Gervais, Canada's Consumer Privacy Protection Act (Bill C-27): Impact for businesses, juin 2021, en ligne : <https://www.blg.com/en/insights/2022/06/canadas-consumer-privacy-protection-act-bill-c27-impact-for-businesses>.

conclusion qu'est parvenue la Cour supérieure du Québec dans un jugement récent[17] ayant autorisé une demande d'action collective contre *Google* : par ses services[18] et outils publicitaires ou d'analyse[19], *Google* procèderait à la collecte et au partage de renseignements personnels d'internautes sans avertissement préalable ni demande de consentement[20], et ce à l'égard de personnes ayant ou non un compte sur la plateforme[21]. Dans cette affaire, la Cour a conclu à l'apparence sérieuse de droit[22] pour, notamment, la responsabilité extracontractuelle de *Google* en vertu de l'article 1457 du Code civil du Québec[23] (ci-après « C.c.Q. ») du fait de la violation de la Loi sur le privé et de la LPRPDE[24]. Autrement dit, la Cour a reconnu que via ses services et outils, *Google* ne semblait ni respecter l'élément *notice*, ni l'élément *choice* des législations québécoise et canadienne de protection des renseignements personnels, remettant ainsi en question la possibilité même de contrôle des internautes sur leurs données. Une décision récente de la Cour suprême de la Colombie-Britannique[25] a aussi reconnu l'absence de consentement d'utilisateurs et d'utilisatrices de *Facebook* quant à l'utilisation de certains de leurs renseignements personnels par le réseau social, le tout en violation des lois de protection de la vie privée de la Colombie-Britannique, du Manitoba, de la Saskatchewan et de Terre-Neuve-et-Labrador[26]. En 2018, un rapport de l'ONG anglaise *Privacy International* mettait déjà de l'avant que les données des personnes pouvaient être collectées par *Facebook* par le biais d'applications tierces même si elles n'avaient pas de compte sur le réseau social et en l'absence de notification suffisante et de consentement préalable (PRIVACY INTERNATIONAL, 2018, p. 28 et 33). La combinaison des données collectées par les applications, puis transférées à *Facebook*, donnait ainsi la possibilité au réseau social de dresser un portrait précis des individus lui permettant de réaliser un démarchage adapté, une adaptation des prix en fonction de leur propension à payer ou encore une proposition de publicité adaptée à leurs envies et préférences. Une démarche de profilage, donc, en l'absence de connaissance et de consentement des internautes.

1.2.2. UN CONSENTEMENT CONTRAINT

[8] Mais même lorsque les données personnelles sont collectées et traitées en connaissance de cause, le consentement est une base légale dangereuse. En effet, face aux géants du numérique, le consentement des personnes sera souvent résigné sous peine de se voir refuser l'accès aux services ou de perdre certains avantages (DELACROIX & LAWRENCE, 2019, p. 249). La forme binaire du consentement (oui ou non) pourrait se résumer à opposer l'individu à la société ou la société à l'individu (STOEKLÉ, DELEUZE, VOGT & HERVÉ, 2017, p. 189; DELACROIX & LAWRENCE,

17 *Option Consommateurs* c. *Google*, 2022 QCCS 2308.

18 *Id.*, par. 23 : « les Services Google […] incluent, entre autres, la recherche sur Internet (Google Search et Images), la cartographie et le guidage routier (Google Maps), les actualités (Google Actualité) et la traduction (Google Traduction). »

19 *Id.*, par. 24 : « les Outils Google […] sont des outils publicitaires ou d'analyse offerts par Google lorsque les membres du groupe naviguent sur des sites Internet qui utilisent ces outils. »

20 *Id.*, par. 30-31, 46, 50 et 54.

21 *Id.*, par. 3.

22 *Id.*, par. 11 et 144.

23 Code civil du Québec, RLRQ, c. CCQ-1991 (ci-après « C.c.Q. »).

24 Sur la violation de la Loi sur le privé, voir *Option Consommateurs* c. *Google*, préc., note 17, par. 62-67. Sur la violation de la LPRPDE, voir les par. 68-70 et 77-81.

25 *Douez* v. *Facebook Inc.*, 2022 BCSC 914.

26 *Id.*, par. 2, 73, 86 et 139.

2019, p. 236). Si les personnes n'acceptent pas le traitement de leurs données personnelles, elles se coupent alors de différents services qui s'avèrent aujourd'hui être une nécessité sociale – trouver un emploi, communiquer avec des ami·es ou des membres de la famille, accéder aux nouvelles ou participer à la vie politique. (BALKIN, 2020, p. 13 ; SWIRE, 2012, p. 1379-1390 ; ALI & UK AI COUNCIL, 2021, p. 32). En 2017, dans *Douez* c. *Facebook*[27], c'est ce que rappelait la Cour suprême du Canada après avoir qualifié de « contrat d'adhésion »[28] la relation liant *Facebook* aux consommateurs :

> Les [personnes désireuses] de participer aux nombreuses communautés en ligne qui communiquent entre elles par l'intermédiaire de Facebook doivent accepter les conditions de l'entreprise ou se résoudre à ne pas faire partie de son réseau social omniprésent. Comme le souligne l'intervenante […] « l'accès à Facebook et aux plateformes de média social […] a vu son importance s'accroître dans l'exercice de la liberté d'expression et de la liberté d'association, ainsi que dans la pleine participation à la démocratie » […] Le choix de « ne pas être en ligne » ne saurait constituer un choix véritable à l'ère d'Internet.[29]

[9] En 2021, c'est d'ailleurs 78 % des Québécois et Québécoises qui utilisaient les réseaux sociaux, une statistique qui grimpe à 90 % et à 91 % chez les 18 à 24 ans et les 25 à 34 ans respectivement (ATN[30], 2022).

[10] Ce consentement non libre est renforcé par le *design* des choix : les interfaces sont conçues de manière à maximiser la collecte de données personnelles (CNIL[31], 2019, p. 10 et 27-30 ; RICHARDS & HARTZOG, 2021, p. 991-992). Un rapport de la CNIL mettait d'ailleurs en avant que « [l]es méthodes utilisées par les concepteurs, à savoir le nudge, les dark patterns ou les designs trompeurs, [agissent] sur [les] comportements et [le] libre-arbitre [des individus] […] [qui] peuvent être amenés à partager toujours plus sans en avoir nécessairement conscience » (CNIL, 2019, p. 14). À titre d'exemple, la page d'inscription de *Facebook* prévoit un unique bouton vert « S'inscrire » qui entraîne acceptation des « Conditions de service », de la « Politique de confidentialité » et de la « Politique d'utilisation des cookies »[32], mentionnées en petits caractères de couleur terne[33]. Face à l'asymétrie de pouvoir existant entre le réseau social et les simples internautes, les personnes ne sont pas en mesure de négocier[34] quelle utilisation sera faite de leurs données et ne peuvent qu'accepter des conditions déjà déterminées (GROUPE D'EXAMEN, 2020, p. 11 ; ALLEN, 2016, p. 72).

27 *Douez* c. *Facebook Inc.*, 2017 CSC 33.

28 *Id.*, par. 53-55.

29 *Id.*, par. 56.

30 Académie de la transformation numérique.

31 Commission nationale de l'informatique et des libertés, France.

32 Meta, Conditions de service, en ligne : <https://www.facebook.com/legal/terms/update>; Meta, Politique de confidentialité, en ligne : <https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect& entry=0>; Meta, Politique d'utilisation des cookies, en ligne : <https://www.facebook.com/policies/cookies/>.

33 Meta, Facebook. Avec Facebook, partagez et restez en contact avec votre entourage., 2022, en ligne : <https://www.facebook.com/>.

34 Également discuté dans *Douez* c. *Facebook Inc*, préc., note 27, par. 52-57.

1.2.3. UN CONSENTEMENT NON ÉCLAIRÉ

[11] Aussi, la complexité des conditions d'utilisation et des technologies en place, l'impossibilité de prévoir les finalités auxquelles les corrélations aboutiront (RICHARDS & HARTZOG, 2019, p. 1479-1486) ou encore la difficulté de prendre le recul nécessaire au moment de presser le bouton « j'accepte », sont tout autant de facteurs rendant le consentement inefficient (POULLET, 2021, p. 96). Pour certains, le consentement n'est plus qu'une fiction inadaptée à la collecte des données personnelles (COMMISSION DE RÉFLEXION[35], 2015, p. 138). De fait, que reste-t-il du consentement éclairé lorsque la majorité des personnes n'ont ni les connaissances, ni les compétences pour comprendre les risques découlant du traitement de leurs données, car non conscientes de leur croisement avec des millions d'autres (FAIRFIELD & ENGEL, 2015, p. 390) ? Une connaissance parcellaire (CNIL, 2019, p. 20) des conséquences et risques liés à la collecte et au traitement des données personnelles pourrait en théorie être acquise par la lecture attentive des conditions d'utilisation et politiques de confidentialité (DELACROIX & LAWRENCE, 2019, p. 249), mais cette pratique se révèle illusoire. Des travaux ont montré que ces documents étaient rarement lus (SOLOVE, 2012, p. 1884) et qu'en prendre connaissance demanderait environ 25 jours de lecture sur un an (CNIL, 2019, p. 20; MCDONALD & CRANOR, 2008). Les personnes ne sont pas conscientes de la valeur de leurs données personnelles, et si elles arrivent à entrevoir de possibles atteintes, leurs conséquences individuelles d'apparence anodines occultent les effets préjudiciables de leur cumul (BEN-SHAHAR, 2019, p. 196-107 ; DELACROIX & LAWRENCE, 2019, p. 237 ; ALI[36] & UK AI COUNCIL, 2021, p. 33 ; O'HARA, 2020, p. 484-485).

1.2.4. UN CONSENTEMENT FICTIF

[12] Enfin, même si le consentement d'une personne pouvait réellement être libre et éclairé, deux problèmes persistent. Le premier est que les plateformes peuvent de toute façon faire fi de la décision des internautes, rendant ineffectifs les effets attendus des mécanismes de notification et de choix :

> […] on aurait pu croire qu'avec l'activation de [la fonction Interdire le suivi], les membres pourraient choisir et indiquer expressément à Google qu'ils ne consentent pas à la collecte et l'utilisation à des fins commerciales de leurs renseignements. Or, […] « la plupart des sites et des services Web (y compris ceux appartenant à Google) ne modifient pas leur comportement lorsqu'ils reçoivent une requête "Interdire le suivi" ». Autrement dit, […] Google ne leur permet finalement jamais de respecter le choix des membres de ne pas voir leurs renseignements collectés par Google.[37]

[13] Le deuxième est que le consentement individuel d'un utilisateur ou d'une utilisatrice est susceptible d'attenter à la vie privée d'autres personnes n'ayant, elles, pas consenti à la collecte ou l'utilisation de leurs données : « [i]n the digital age, everyone is always informing on everyone else. Thus, an individual's response to a notice-and-choice regime may affect the privacy of many other people who have no say in the matter. » (BALKIN, 2020, p. 17).

35 Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique, France.

36 Ada Lovelace Institute, Angleterre.

37 *Option Consommateurs* c. *Google*, préc., note 17, par. 52.

2. VERS UNE APPROCHE COLLECTIVE DE LA VIE PRIVÉE

[14] À l'ère de l'hyperconnexion du monde, les données personnelles sont devenues des « données en réseaux » (BOURCIER & DE FILIPPI, 2018, p. 452) ou des « données relationnelles » (CNIL, 2020, p. 32), qui lient plusieurs personnes entre elles. Les choix d'une personne dans l'environnement numérique font intervenir la vie privée d'autrui. Ce problème est particulièrement présent sur les réseaux dits « sociaux », qui cherchent à mettre en relation les internautes et à les inciter à partager leur vie sociale, laquelle implique inévitablement d'autres individus. Nous pouvons penser à l'internaute qui publie une photo et qui y mentionne d'autres personnes, ou encore au membre d'un réseau social qui commente le nom de son ami·e sous une publication pouvant l'intéresser. Au-delà de ces cas de figure, les conséquences sur la vie privée d'autrui tiennent aujourd'hui au fait que le traitement de données générées par les activités en ligne d'une personne et d'apparence anodines permet de découvrir des informations précises sur elle (DÉZIEL, 2018, p. 834s), mais aussi sur les personnes avec lesquelles elle est connectée ou avec lesquelles elle présente des similarités (BALKIN, 2020, p. 17-18). Dès lors, le modèle de *notice and choice* suppose à tort une approche individuelle de la vie privée selon laquelle chaque personne gère des informations uniquement propres à elle-même. L'internaute qui consent à la collecte et à l'utilisation de ses données personnelles par une plateforme devient un vecteur d'informations sur l'ensemble des membres de son réseau, que ces personnes aient consenti ou non à la collecte de leurs renseignements personnels et qu'elles soient membres ou non d'un réseau social (VÉLIZ, 2019). S'inscrire sur une plateforme en ligne n'est pas un choix purement individuel, mais bien un choix collectif. Dès lors, il semble nécessaire de mettre en œuvre une nouvelle façon de gérer les données personnelles : une façon collective, dans l'intérêt de toutes et tous.

▪ Bien commun, ressource collective, gestion collective

[15] Face aux limites de la conception individualiste de la vie privée, des autrices et auteurs ont réfléchi à la vie privée à partir de sa dimension sociale. Sur la base de théories économiques, certains ont articulé des propositions concevant les données comme un bien commun (FAIRFIELD & ENGEL, 2015 ; SAETRA, 2020). Dans la même veine, d'autres ont envisagé les données comme une ressource commune ou collective (SAVAGE, 2019). Au Québec, c'est le cas du professeur Trudel, qui a écrit en faveur d'une réglementation des données personnelles « comme une ressource collective, non comme une addition de renseignements portant sur des individus »[38]. Les mécanismes de gestion collective des données, tels que les fiducies de données, les coopératives de données ou les *data commons*, ont fait l'objet d'une littérature de plus en plus abondante (DELACROIX & LAWRENCE, 2019 ; MOZILLA INSIGHTS, van GEUNS et BRANDUSESCU, 2020 ; ALI & UK AI COUNCIL, 2021).

38 Voir notamment la chronique de P. TRUDEL, « La valeur de nos données personnelles », Le Devoir, 13 mars 2018, en ligne : <https://www.ledevoir.com/opinion/chroniques/522496/la-valeur-de-nos-donnees-personnelles>.

[16] Il s'agit pour nous de faire l'examen critique de deux pistes de solutions juridiques potentielles ancrées dans une conception collective de la vie privée. Nous traitons d'abord des fiducies de données et de leur possible appréhension par le droit commun québécois, pour ensuite nous tourner vers les obligations fiduciaires de *common law* qui peuvent naître indépendamment de la constitution d'une fiducie. Nous examinons plus spécifiquement le devoir de loyauté. Cette deuxième solution nous paraît plus adéquate pour remédier aux problèmes identifiés auxquels les lois actuelles de protection des renseignements personnels ne parviennent pas à répondre, mais soulève tout de même des difficultés importantes.

2.1. LES FIDUCIES DE DONNÉES

[17] Cette section procède en quatre temps. Nous expliquons d'abord le fonctionnement général du mécanisme de fiducie en droit canadien et en droit québécois. Nous définissons ensuite le concept de fiducie de données. Par après, nous montrons que le cadre flexible des dispositions sur la fiducie du droit commun québécois[39], et plus particulièrement son concept de fiducie d'utilité sociale, pourrait en théorie permettre d'opérationnaliser les fiducies de données (HULIN, 2020; LEBLANC, 2020 ; LEBLANC, 2021). Enfin, nous exposons certains avantages et inconvénients des fiducies de données, ces derniers militant selon nous en défaveur de leur reconnaissance comme solution réaliste pour faire face à l'asymétrie de pouvoir et d'information existant entre les plateformes et les internautes, et à ses effets.

2.1.1. LE MÉCANISME DE LA FIDUCIE EN DROIT QUÉBÉCOIS ET CANADIEN

[18] La fiducie est un instrument juridique dont les origines remontent au droit romain et qui s'est concrétisé dans les juridictions de *common law*, principalement en Angleterre, sur la base des principes de l'*equity* (« Court of Chancellery ») (O'HARA, 2020, p. 484 ; GRENON, 2006, p. 88 ; LEBLANC, 2021 p. 5). La fiducie fait généralement intervenir trois acteurs : le constituant, le bénéficiaire et le fiduciaire. Le mécanisme a traditionnellement été utilisé pour attribuer la propriété et le pouvoir de gestion d'un bien à une personne (fiduciaire), cette dernière devant veiller à conserver et à utiliser ce bien en conformité avec les objectifs déterminés par le constituant et au profit d'une ou de plusieurs personnes (bénéficiaires).

[19] La fiducie québécoise, dont la dernière mouture a été codifiée en 1994 aux articles 1260 à 1298 C.c.Q., tire ses origines du droit anglais des *trusts*[40], mais s'en distingue à plusieurs niveaux. En vertu du C.c.Q., la fiducie résulte de la manifestation expresse de volonté des constituant et fiduciaire[41] (GILLEN & al, 2021, p. 777-778 et 790). Son article 1260 dispose en effet que la fiducie est créée à la suite d'un acte où le constituant « transfère de son patrimoine à un autre patrimoine qu'il constitue, des biens qu'il affecte à une fin particulière et qu'un fiduciaire s'oblige […] à détenir et à administrer ». L'article 1261 C.c.Q. consacre quant à lui le caractère autonome du

39 Art. 1260-1298 C.c.Q.

40 *Royal Trust Co.* c. *Tucker*, (1982) 1 R.C.S. 250, p. 261.

41 Art. 1260, 1262 et 1264 al. 1 C.c.Q.

patrimoine d'affectation. Aucun des trois acteurs n'a donc de droit réel, et donc de droit de propriété, sur le bien détenu en fiducie. Le rôle du fiduciaire est assimilable à celui de l'administrateur du bien d'autrui chargé de la pleine administration[42]. La fiducie québécoise peut notamment être établie par contrat ou par la loi et est constituée dès qu'acceptée par le fiduciaire[43]. C'est à ce moment que ses obligations envers le ou les bénéficiaires naissent[44]. Le C.c.Q. crée trois types de fiducies[45], catégorisées en fonction de leur finalité particulière (GRENON, 2006, p. 89). On y retrouve notamment la fiducie d'utilité sociale[46]. Le droit canadien de *common law* a quant à lui permis le développement d'un droit des fiducies (*trusts*) beaucoup plus complexe et comportant de nombreuses ramifications (GILLEN & al, 2021, p. 12). Les fiducies de *common law* sont classées selon leur mode de constitution (GRENON, 2006, p. 89) : les fiducies de plein droit (« trusts by operation of law »), les fiducies statutaires et les fiducies expresses (GILLEN, 2021, p. 12). Dans la *common law* canadienne, à l'inverse du droit civil québécois, le fiduciaire se voit confier la propriété sur le bien détenu pour être en mesure d'exercer ses obligations. Dans les deux systèmes juridiques[47], la constitution d'une fiducie fait naître des devoirs de loyauté, de prudence et de diligence qui incombent au fiduciaire (GILLEN & al, 2021, p. 67 et 70 ; LEBLANC, 2021, p. 15).

2.1.2. LA NOTION DE FIDUCIE DE DONNÉES

[20] L'idée des fiducies de données (*data trusts*) a émergé en 2004 (EDWARDS, 2004) et a été popularisée en 2016 par Neil Lawrence[48] dans un contexte de protection des consommateurs (O'HARA, 2020, p. 488). Les fiducies de données ont notamment été envisagées comme une solution prometteuse pour atténuer le déséquilibre de pouvoir prévalant entre les grands collecteurs de données et les personnes (DELACROIX & LAWRENCE, 2019, p. 240; RINIK, 2020, p. 342-359). Leur fonctionnement se calque sur les mécanismes juridiques existants. L'idée générale est de confier la gestion des données d'un groupe de personnes à un fiduciaire (WYLIE & MCDONALD, 2018), qui est alors tenu à des obligations de loyauté, de prudence et de diligence (LEBLANC, 2021, p. 5; ELEMENT AI & NESTA, 2019, p. 14). Dans les propositions de 2018 de modernisation de la LPRPDE, le fonctionnement de la fiducie de données emprunte aux *trusts* de *common law* en traitant du transfert de la propriété légale au fiduciaire[49].

▪ Les fiducies de données pour remédier à l'*undersharing* et à l'*oversharing* de données

[21] Envisagée comme un outil permettant une gouvernance responsable des renseignements personnels, la fiducie de données serait à même de remédier aux problèmes issus du sur-partage (*oversharing*) et du sous-partage (*undersharing*) de données (HOUSER & BAGBY, 2022, p. 1, 5-8, 19 et 51). Ainsi, dans les propositions de

42 Art. 1278 al. 2, 1299 et 1306-1307 C.c.Q.

43 Art. 1262 et 1264 al. 1 C.c.Q

44 Art. 1265 C.c.Q.

45 Art. 1266 al. 1 C.c.Q.

46 Art. 1270 C.c.Q.

47 En droit québécois, voir les articles 1278 al. 2 et 1309 C.c.Q.

48 N. Lawrence « Data Trusts Could Allay our Privacy Fears », The Guardian, 3 juin 2016, en ligne : <https://www.theguardian.com/media-network/2016/jun/03/data-trusts-privacy-fears-feudalism-democracy>.

49 Gouvernement du Canada, ministère Innovation, Sciences et Développement économique Canada.

2018 de modernisation de la LPRPDE (GOUV. CAN., 2019), la fiducie de données était présentée comme une solution émergente susceptible de favoriser le partage et l'utilisation sécuritaire des données aux fins de recherche et d'innovation, notamment dans le domaine de la santé. On y présentait entre autres la possibilité d'établir un régime d'utilisation désidentifié des données au sein de la loi afin que l'information soit traitée sans le consentement individuel des personnes concernées lorsque leurs renseignements étaient confiés en fiducie. Par exemple, des personnes souffrant d'une maladie rare pourraient être incitées à confier en fiducie leurs renseignements personnels sensibles, autrement inaccessibles, dans l'objectif socialement bénéfique de faire avancer la recherche et les connaissances sur cette maladie (ELEMENT AI & NESTA, 2019, p. 25 ; HOUSER & BAGBY, 2022, p. 46). Lawrence et Delacroix (2019) ont de leur côté défendu une conception dite « ascendante » des fiducies de données (« bottom-up data Trusts »), calquée sur le fonctionnement des fiducies expresses de *common law*, où les personnes pourraient choisir de mettre en commun les droits qu'elles ont sur leurs données personnelles de manière à recalibrer les rapports de force existant entre elles et les grands collecteurs de données et, partant, à freiner les problèmes issus du sur-partage de renseignements personnels aux géants du numérique. Selon cette conception, les constituants de la fiducie pourraient également en être les bénéficiaires et il serait souhaitable de chercher à mettre en place un « écosystème » de fiducies de données, où l'offre variée de fiducies privées, publiques et spécialisées permettrait aux personnes de choisir l'instrument répondant le mieux à leurs attentes en matière de vie privée (DELACROIX & LAWRENCE, 2019, p. 240-241 et 247).

2.1.3. LA FIDUCIE D'UTILITÉ SOCIALE DU C.C.Q POUR OPÉRATIONNALISER LA FIDUCIE DE DONNÉES

[22] La fiducie d'utilité sociale du C.c.Q., codifiée à l'article 1270 C.c.Q. et visant la réalisation d'un objectif d'intérêt général, pourrait servir à opérationnaliser la fiducie de données (HULIN, 2020; LEBLANC, 2020, p. 3-7; LEBLANC, 2021, p. 21-24)[50]. Appliquée en contexte numérique, elle permettrait de rétablir l'équilibre entre les internautes et les plateformes en ligne, en ce que sa vocation serait d'apporter une protection effective du droit à la vie privée en faisant en sorte que les données des internautes soient collectées et traitées conformément à cette finalité (LEBLANC, 2020, p. 5)[51].

▪ La qualification des données comme biens et le patrimoine d'affectation du C.c.Q

[23] L'article 1261 C.c.Q. dispose que le patrimoine fiduciaire est formé lorsque les biens sont transférés en fiducie. Le statut juridique des données personnelles est toutefois source de débat (MOURON, 2018). En insistant sur leur dimension personnelle et en les appréhendant avant tout comme des éléments rattachés à la personnalité, des autrices se sont opposées à leur reconnaissance comme biens et à

50 Étant donné notre objectif d'examiner des solutions s'ancrant dans une gestion collective des données, nous ne nous penchons pas sur les fiducies à des fins personnelles ou à des fins d'utilité privée (art. 1266 C.c.Q.). Les premières doivent fournir un avantage direct à une personne spécifique, déterminée ou déterminable (art. 1267 C.c.Q) et sont limitées dans le temps (art. 1271 al. 1 C.c.Q.). Les secondes se rapportent à un intérêt de nature privée (art. 1268 C.c.Q.) Ainsi, il nous semble que la fiducie d'utilité sociale « constituée dans un but d'intérêt général » (art. 1270 C.c.Q.) soit particulièrement adaptée à l'objectif de protection de la vie privée.

51 Art. 1287s, 1299 et 1306s C.c.Q.

leur patrimonialisation (ROCHFELD, 2015 ; VAAST, 2021). Or, si les données relèvent de la personne, leur potentiel de monétisation les fait également entrer dans la catégorie de « l'avoir », ou du moins, de la « chose » (MOURON, 2018, p. 2). En discutant de la qualification juridique des données, HULIN (2020) insistait d'ailleurs sur leur valeur économique et sur le fait qu'elles soient à la base des pratiques commerciales de plusieurs entreprises – rappelons que les plateformes en ligne génèrent de la valeur à partir du traitement d'une quantité massive de données issues de l'activité en ligne des internautes. En affirmant la possibilité en droit de la constitution d'un patrimoine dans le contexte de la fiducie de données et en s'appuyant sur van ERP (2020), elle soulignait d'ailleurs que « les enjeux théoriques de qualification n'ont pas empêché le développement d'un marché international des données, y compris à caractère personnel ».

[24] Le patrimoine d'affectation du C.c.Q. nous semble par ailleurs particulièrement adapté à la fiducie de données. Contrairement aux fiducies de *common law*, il évacue la notion de droit de propriété[52] (LEBLANC, 2021, p. 14, 19 et 21-22 ; GILLEN & al, 2021, p. 760-761). La conception de la fiducie du droit québécois répond donc à l'une des principales objections soulevées dans un rapport commandé par le *Open Data Institute* (ci-après « ODI »), qui avait remis en question la compatibilité des *trusts* de *common law* avec les données[53]. D'ailleurs, la définition de fiducie de données proposée par l'ODI, soit « [a] legal structure that provides independent third-party stewardship of data »[54], est une conception du mécanisme déjà retenue dans le C.c.Q.

- Les mécanismes de surveillance et la flexibilité du mécanisme

[25] Le C.c.Q. prévoit aussi des mesures de surveillance et de contrôle qui s'appliquent au fiduciaire en tant qu'administrateur du bien d'autrui[55]. Ces règles peuvent se transposer à un contexte de fiducie de données (HULIN, 2020). Par exemple, les constituants, bénéficiaires ou toute personne intéressée, peuvent saisir le tribunal pour contraindre le fiduciaire à exécuter ses obligations ou à s'abstenir d'exécuter une action dommageable à l'objectif de la fiducie[56]. Les articles 1310 à 1314 C.c.Q. prévoient quant à eux que le fiduciaire ne peut se trouver en conflit d'intérêts. Enfin, si le droit des *trusts* de *common law* se caractérise par sa flexibilité pour répondre à différentes situations (ALI & UK AI COUNCIL, 2021, p. 37), les règles du droit civil québécois des fiducies sont décrites comme étant dotées d'une « élasticité extraordinaire » (PICCINI ROY, 2010, p. 343 ; GILLEN, 2021, p. 756), se voulant donc d'autant plus adaptées pour trouver application dans une variété de contextes découlant des évolutions rapides en société (LEBLANC, 2021, p. 23-24).

52 Art. 915 et 1261 C.c.Q.

53 BPE Solicitors, Pinsent Masons et C. Reed, Data trusts: legal and governance considerations, avril 2019, en ligne : <https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf>.

54 Open Data Institute, « Defining a 'data trust' », Open Data Trust, 19 octobre 2018, en ligne : <https://theodi.org/article/defining-a-data-trust/>.

55 Art. 1287-1292 C.c.Q.

56 Art. 1290 al. 1 C.c.Q.

2.1.4. LES AVANTAGES DES FIDUCIES DE DONNÉES DANS LE CONTEXTE DES PLATEFORMES EN LIGNE

[26] Dans le contexte d'une relation entre une plateforme en ligne et les internautes, le mécanisme de fiducie permet au fiduciaire chargé de la gestion des données de faire valoir les droits individuels, sur la base des lois existantes, des bénéficiaires. Il s'agit là d'un point positif essentiel dans un contexte où ces droits sont autrement rarement invoqués par les internautes – par manque de temps, de ressources, ou simplement en raison de la méconnaissance de ces droits ou de la banalité des conséquences individuelles résultant de la collecte et du traitement des données (DELACROIX & LAWRENCE, 2019, p. 238). Du fait de la délégation du consentement individuel au fiduciaire, les fiducies de données présentent l'avantage de la négociation collective (WYLIE & MCDONALD, 2018 ; ALI & UK AI COUNCIL, 2021, p. 35 ; HOUSER & BAGBY, 2022, p. 25) de ce que l'on pourrait appeler le « métaconsentement » (HULIN, 2020; PLOUG & HOLM, 2015) du fiduciaire, ce dernier étant en bien meilleure posture pour apprécier la portée, les risques et la conformité légale de la collecte et du traitement des données. Le fiduciaire peut donc veiller à l'utilisation responsable des données, conformément à l'objectif de la fiducie, sans devoir obtenir de façon répétée le consentement des personnes (LEBLANC, 2021, p. 23). Le mécanisme permettrait donc de rééquilibrer les relations de pouvoir entre internautes et géants du web : plus les internautes mettent leurs données personnelles en commun, plus le fiduciaire est apte à faire pencher la balance en leur faveur.

- Le devoir indivisible de loyauté et l'offre variée de fiducies

[27] Les fiduciaires de données ne peuvent pas se trouver en conflit d'intérêts, contrairement aux plateformes en ligne qui ont avantage à faire prévaloir les intérêts de leurs actionnaires, et donc à valoriser les données de leurs utilisateurs et utilisatrices sans tenir compte de leurs intérêts opposés (MOZILLA INSIGHTS, van GEUNS & BRANDUSESCU, 2020, p. 13). Ici, toutefois, le devoir « indivisible » de loyauté des fiduciaires les empêche de faire prévaloir des intérêts autres que ceux des bénéficiaires (DELACROIX & LAWRENCE, 2019, p. 241; O'HARA, 2020, p. 488; ALI & UK AI COUNCIL, 2021, p. 35). Les personnes peuvent aussi être rassurées quant à l'utilisation de leurs données en conformité avec l'objet de la fiducie, en ce que les fiduciaires peuvent être tenus personnellement responsables en cas de fraude à ce devoir[57] (LEBLANC, 2021, p. 22). Enfin, la concurrence créée par une offre variée de fiducies de données maximise la protection de la vie privée et permet aux personnes de faire le choix du mécanisme satisfaisant leurs préférences (ELEMENT AI & NESTA, 2019, p. 30).

57 Pour le cas de la fiducie québécoise, voir par exemple l'article 1292 C.c.Q.

2.1.5. LES DIFFICULTÉS DES FIDUCIES DE DONNÉES DANS LE CONTEXTE DES PLATEFORMES EN LIGNE

- Le retour de la conception individualiste de la vie privée

[28] Les fiducies de données demeurent basées sur une approche individualiste de la vie privée, en ce que le mécanisme repose toujours sur le choix personnel des internautes de confier la gestion de leurs données à un fiduciaire. Resurgissent donc les difficultés associées au modèle de *notice and choice* détaillées précédemment. Si le modèle fiduciaire trouve son utilité dans l'idée que les personnes sont incapables d'offrir un consentement éclairé aux grandes entreprises qui collectent et traitent leurs données, il suppose simultanément leur capacité à comprendre un outil juridique émergent, abstrait et complexe nécessitant la lecture de tout autant de politiques d'utilisation et de confidentialité des données (LEBLANC, 2021, p. 24 ; O'HARA, 2021, p. 489). Cette difficulté est exacerbée en présence d'une offre variée de fiducies de données, laquelle reproduit les difficultés du consentement à l'étape du choix de la fiducie. L'asymétrie d'information initiale se retrouve transposée entre les internautes et les fiduciaires : « it should be noted that information asymmetries could also exist between individuals and trusts, not only between individuals and organisations. » (ALI & UK AI COUNCIL, 2021, p. 41).

- La compromission de la vie privée d'autrui et la difficulté de (re)prise de contrôle

[29] Les personnes qui choisissent de ne pas avoir recours à une fiducie peuvent par ailleurs compromettre tant leur vie privée que celle des autres, étant donné la nature relationnelle des données décrite précédemment. Et si elles font le choix de la fiducie, le problème inverse se pose, en ce qu'elles consentent alors à confier leurs propres renseignements, mais aussi ceux d'autres personnes n'ayant pu apposer leur accord : « [b]y consenting […] a user becomes a conduit for gathering information about her entire social network, whether or not they have consented. » (FAIRFIELD & ENGEL, 2015, p. 410). Des difficultés similaires se manifestent si les personnes souhaitent retirer leurs données de la fiducie. Comment « retrouver » les données se rapportant à une personne en particulier sans affecter le choix d'une autre ? Même dans l'hypothèse où les personnes mettraient en commun leurs droits sur les données, il faudrait être en mesure de rattacher ces droits individuels aux renseignements en question, ce qui soulève le même problème. Il faut aussi dire que la collecte de données par les plateformes en ligne n'en est plus du tout à ses débuts (MARINOTTI, 2022, p. 23). Il semble alors difficile de concevoir la manière dont les fiducies de données pourraient permettre de retrouver un contrôle effectif sur des millions de données déjà disséminées – et sur les informations inférées à partir de leur traitement.

- Le manque d'acteurs clés

[30] La mise en application pratique des fiducies de données semble aussi compromise par le manque d'incitatifs pour attirer des fiduciaires (O'HARA, 2020, p. 489 ; ALI & UK AI COUNCIL, 2021, p. 43-44). De fait, quel acteur voudrait prendre le risque d'engager sa responsabilité pour avoir failli à respecter l'objectif de la fiducie et à maximiser l'intérêt des bénéficiaires, surtout dans un contexte où il ne peut retirer de bénéfices de

sa gestion (O'HARA, 2020, p. 489), où les données lient plusieurs personnes entre elles et où il peut être particulièrement ardu de saisir la portée de ce que constitue une donnée personnelle (MARINOTTI, 2022, p. 15-18)? Aussi, comment s'entendre sur une définition commune de la vie privée et sur la meilleure façon de gérer les données pour la protéger ? Le manque de personnes intéressées à confier leurs données compromet aussi l'existence de la fiducie. Le mécanisme est peu connu (ALI & UK AI COUNCIL, 2021, p. 44) et les personnes peuvent être méfiantes quant au fait qu'un acteur externe veuille gérer leurs renseignements personnels (LEBLANC, 2021, p. 6). À titre d'exemples et dans des contextes différents, l'on peut penser au tollé soulevé par la proposition du gouvernement québécois à l'automne 2020 quant à l'utilisation de données médicales de la Régie de l'assurance maladie du Québec (RAMQ), même si anonymisées, par des compagnies pharmaceutiques à des fins de recherche[58] ou à l'abandon de l'application COVI de notification de contacts de Covid-19 de l'Institut québécois d'intelligence artificielle (MILA) (ALSDURF et al, 2020) par le gouvernement canadien, notamment en raison des inquiétudes quant à la collecte de données personnelles démographiques et de santé[59]. Dans le même ordre d'idées, il faut dire qu'une majorité de Canadiens et de Canadiennes sont préoccupés par la protection de leur vie privée (CPVP, 2021, figure 3) et jugent que les organisations ne respectent pas ce droit (CPVP, 2019b). Dans le cadre d'un sondage commandé par le CPVP, plusieurs ont affirmé avoir refusé de fournir leurs données personnelles à une entreprise ou à une organisation pour des motifs liés à la protection de leur vie privée (CPVP, 2021, figure 12). La confiance des personnes dans un système comme les fiducies de données semble ainsi loin d'être acquise, particulièrement dans un contexte social marqué par divers scandales liés à la compromission de données personnelles[60] et par un déficit de confiance des personnes dans les acteurs, publics et privés, qui utilisent les données (ALI & UK AI COUNCIL, 2021, p. 17).

▪ Les lacunes de la proposition « d'écosystème » de fiducies de données

[31] Le manque de fiduciaires et de personnes désireuses de confier leurs renseignements en fiducies de données remet aussi en question la possibilité « d'écosystème » de fiducies, à la base de la proposition de 2019 de Delacroix et Lawrence (O'HARA, 2020, p. 490 ; ALI & UK AI COUNCIL, 2021, p. 43). Néanmoins, la matérialisation d'un tel écosystème serait à même d'entraîner deux problèmes. Nous percevons d'abord un risque de discrimination à court terme, en ce que les fiducies les plus protectrices de la vie privée pourraient être plus coûteuses[61] que les fiducies de base, plus accessibles et moins chères, mais moins protectrices. Un écosystème de fiducies de données pourrait donc être porteur d'inégalités, en conditionnant une

58 B. Barbeau, « Les données de la RAMQ pour appâter les pharmaceutiques », Radio-Canada Info, 21 août 2020, en ligne : <https://ici.radio-canada.ca/nouvelle/1728106/pierre-fitzgibbon-compagnies-pharmaceutiques-donnes-medicales-mila>; A.-S. Hulin et A. Cossé « Pour une fiducie de données à la RAMQ », Le Devoir, 1er septembre 2020, en ligne : <https://www.ledevoir.com/opinion/idees/585113/pour-une-fiducie-de-donnees-a-la-ramq>.

59 D. Jung, « COVID-19 : l'application de traçage du Mila mise au placard par Ottawa », Radio-Canada Info, 10 juin 2020, en ligne : <https://ici.radio-canada.ca/nouvelle/1710961/coronavirus-tracage-application-mila-canada>; F. Deglise, « Ottawa dit non à Mila et son application COVI de recherche de contacts de personnes contaminées », Le Devoir, 10 juin 2020, en ligne : <https://www.ledevoir.com/societe/580507/ottawa-dit-non-a-mila>.

60 S. Grammond, « Desjardins, Capital One, TransUnion, et après ? », La Presse, 17 octobre 2019, en ligne : <https://www.lapresse.ca/elections-federales/2019-10-17/desjardins-capital-one-transunion-et-apres>.

61 Puisque les fiduciaires ne peuvent tirer des bénéfices de la fiducie, il faudrait en effet que les bénéficiaires paient pour la protection de leurs renseignements personnels. Il s'agit là d'un autre inconvénient des fiducies de données. Est-ce que les personnes seraient prêtes à payer pour une protection, abstraite, de leur vie privée?

protection optimale de la vie privée au statut socio-économique des personnes. À plus long terme, les fiducies de données répliqueraient le problème initial d'asymétrie de pouvoir : les fiducies les plus populaires prendraient progressivement le dessus sur celles ayant attiré moins de personnes. On se retrouverait encore une fois en présence de quelques acteurs dominants, alors que la pertinence et raison d'être des fiducies de données résidaient justement dans l'idée de mettre fin à l'asymétrie de pouvoir existant entre les personnes et les collecteurs de données (O'HARA, 2020, p. 490-491).

▪ La difficulté de surveillance des actions des fiduciaires

[32] Enfin, même si les fiducies de données étaient mises en œuvre, la possibilité concrète de surveillance des actions des fiduciaires est questionnable. L'idée que des internautes puissent être en mesure de surveiller la prise de décision et les comportements des fiduciaires, puis d'identifier les fautes de ces derniers en matière de transactions complexes de données, paraît peu plausible (ALI & UK AI COUNCIL, 2021, p. 43).

2.2. LES OBLIGATIONS FIDUCIAIRES ET LE DEVOIR DE LOYAUTÉ

[33] Cette section examine la possibilité d'assujettir les plateformes en ligne à un devoir fiduciaire de loyauté. Premièrement, nous abordons brièvement les contextes d'émergence des obligations fiduciaires et leur contenu général en droit canadien de *common law*. Deuxièmement, en nous appuyant notamment sur la proposition de GUEVARA (2021), nous énonçons les critères jurisprudentiels donnant ouverture à la reconnaissance d'une relation fiduciaire *ad hoc* et montrons à notre tour qu'une interprétation libérale de ces critères peut servir de base légale à la qualification de la relation entre les plateformes et leurs membres comme étant fiduciaire. Finalement, nous décrivons le devoir fiduciaire de loyauté qui pourrait s'appliquer aux plateformes et abordons les avantages et les difficultés liés à sa mise en œuvre en droit canadien.

2.2.1. LES CONTEXTES D'ÉMERGENCE DES OBLIGATIONS FIDUCIAIRES

[34] Traditionnellement, les obligations fiduciaires résultaient uniquement de la reconnaissance de fiducies légales par les tribunaux jugeant en *equity* (ELLIS & al, 1996, p. 1-1). Lorsqu'une personne se voyait confier la propriété d'un bien pour le compte et pour le seul bénéfice d'une autre personne, les tribunaux pouvaient reconnaître une relation fiduciaire à laquelle était assortie trois grandes obligations spécifiques visant à assurer la protection du bien au profit de cette personne (ELLIS & al, 1996, p. 1-1 ; GILLEN & al, 2021, p. 249 et 338) : un devoir de détenir les biens selon les conditions de constitution de la fiducie, un devoir de loyauté et un devoir de diligence (*duty of care*). On parlait alors de « property being held on trust » (GILLEN & al, 2021, p. 13). Les obligations fiduciaires ont toutefois trouvé application dans des contextes de plus en plus nombreux en raison de la nature particulière de certaines relations et indépendamment de l'existence d'une fiducie et de la notion de propriété (ELLIS & al, 1996, p. 1-1 et 1-2 ; GILLEN & al, 2021, p. 5, 13 et 339s; LEBLANC, 2021, p. 13). En droit canadien, les tribunaux ont ainsi reconnu plusieurs catégories de

relations fiduciaires de fait, comme les relations médecin-patient[62], avocat-client[63] ou administrateur-société[64]. Ils ont aussi développé des critères visant à identifier les relations fiduciaires ponctuelles ou *ad hoc*[65]. Dans ce dernier cas, les trois obligations fiduciaires traditionnelles ne sont pas d'application systématique. Le contexte factuel spécifique de la relation détermine leur existence, mais aussi leur portée[66] (GILLEN & al, 2021, p. 683-686 ; SCOTT, 1949, p. 541).

2.2.2. LES RELATIONS FIDUCIAIRES *AD HOC* EN DROIT CANADIEN ET LES PLATEFORMES EN LIGNE

[35] La reconnaissance de toute relation fiduciaire exige qu'une partie ait placé sa confiance en une autre et que cette dernière ait accepté d'agir conformément à la confiance qui lui était accordée (ELLIS & al, 1996, p. 1-2 ; GILLEN & al, 2021, p. 13 et 339 ; LITMAN, 2006). La Cour suprême a mis en évidence quatre facteurs cumulatifs permettant de conclure à l'existence d'une relation fiduciaire dite *ad hoc*[67] : l'existence d'une personne ou d'un groupe de personnes vulnérables au contrôle du fiduciaire présumé (1), la possibilité pour le fiduciaire présumé d'exercer un pouvoir discrétionnaire ou un contrôle (2) susceptible d'affecter défavorablement un « intérêt juridique ou un intérêt pratique important »[68] de cette ou de ces personnes (3) et une entente mutuelle ou un engagement exprès ou implicite[69] du fiduciaire présumé à agir dans le meilleur intérêt de l'autre partie (4). GUEVARA (2021) montre que ces critères peuvent servir de base légale à la qualification de la relation entre les plateformes en ligne et leurs utilisateurs et utilisatrices comme étant fiduciaire. Nous souscrivons à sa proposition. Nous en faisons également la démonstration en mettant de l'avant certaines pratiques des plateformes en ligne et en rappelant des éléments discutés en première partie d'article. Nous optons toutefois pour une vision élargie du critère de l'intérêt juridique ou pratique important de manière à tenir compte des intérêts collectifs.

2.2.2.1. LA VULNÉRABILITÉ DES UTILISATEURS ET DES UTILISATRICES

[36] La vulnérabilité des utilisateurs et des utilisatrices découle des asymétries de pouvoir et d'information détaillées précédemment (BALKIN, 2020, p. 11-12; ALI & UK AI COUNCIL, 2021, p. 24). La collecte massive de données personnelles et leur traitement permet d'inférer des informations que les personnes n'ont pas voulu révéler, qu'elles ne savent probablement pas avoir été découvertes et dont l'exploitation peut desservir leurs intérêts (DELACROIX & LAWRENCE, 2019, p. 239 ; KRÖGER & al, 2021). Cette vulnérabilité est par ailleurs exacerbée par la méconnaissance de ces risques (SOLOVE, 2020 p. 25) et par la dépendance des personnes aux plateformes, devenues des outils presque essentiels à la vie en société. Au sens du droit canadien de *common*

62 Par exemple : *Norberg* c. *Wynrib*, (1992) 2 R.C.S. 226, p. 230; *McInerney* c. *MacDonald*, (1992) 2 R.C.S. 138, p. 139.

63 Par exemple : *Strother* c. *3464920 Canada Inc.*, 2007 CSC 24, par. 34-35.

64 *Alberta* c. *Elder Advocates of Alberta Society*, 2011 CSC 24, par. 33; *Can. Aero* c. *O'Malley*, (1974) R.C.S. 592.

65 Sur l'évolution des critères donnant ouverture à la reconnaissance d'une relation fiduciaire *ad hoc* : *Frame* c. *Smith*, (1987) 2 R.C.S. 99; *Lac Minerals Ltd.* c. *International Corona Resources Ltd.*, (1989) 2 R.C.S. 574; *Hodgkinson* c. *Simms*, (1994) 3 R.C.S. 377; *Galambos* c. *Perez*, 2009 CSC 48; *Alberta* c. *Elder Advocates of Alberta Society*, préc., note 64; Gillen & al, (2021), p. 668-682.

66 *Alberta* c. *Elder Advocates of Alberta Society*, préc., note 64, par. 33.

67 *Id.*, par. 36.

68 *Id.*, par. 35-36.

69 *Galambos* c. *Perez*, préc., note 65, par. 66.

law, les internautes sont vulnérables car « [incapables] d'empêcher l'exercice abusif du pouvoir discrétionnaire »[70] par les plateformes, mais aussi parce qu'ils ne disposent pas de recours appropriés en cas d'exploitation abusive de leurs données[71]. À cet effet, notons qu'au Canada, les plateformes peuvent actuellement faire fi des conclusions et recommandations du CPVP[72] même lorsqu'il est reconnu que des infractions ont été commises (CPVP, 2019a et 2019b)[73].

2.2.2.2. LE POUVOIR DISCRÉTIONNAIRE EXERCÉ PAR LES PLATEFORMES

[37] Le pouvoir discrétionnaire des plateformes s'exerce sur leurs utilisateurs et utilisatrices par le biais de techniques de profilage, de *nudging* (THALER & SUNSTEIN, 2008), et ultimement de manipulation (RICHARDS & HARTZOG, 2021, p. 976). À partir de techniques de sciences des données et d'une collecte massive d'informations sur leurs membres, les plateformes sont en mesure de les répartir en différents groupes algorithmiques (DÉZIEL, 2018, p. 838-839 ; DU PERRON, 2020, p. 37), mieux prédire leur comportement et ainsi leur présenter du contenu susceptible de capter leur attention à un moment précis. En empruntant aux sciences cognitives et comportementales dans leur *design*, elles maîtrisent la façon dont les choix sont faits (RICHARDS & HARTZOG, 2021 ; ALI & UK AI COUNCIL, 2021, p. 33). Exploitant ainsi les biais cognitifs des internautes (CNIL, 2019, p. 15 et 27), les plateformes exercent un pouvoir sur la prise de décisions des personnes, qui « choisissent » de demeurer longtemps en ligne et de cliquer aux endroits vers lesquels elles sont guidées, fournissant ainsi toujours plus de données personnelles (BALKIN, 2020, p. 16 ; CNIL, 2019, p. 14). En combinant les techniques de profilage à celles de *nudging*, les plateformes en viennent à exercer un véritable pouvoir sur le comportement de leurs membres (RICHARDS & HARTZOG, 2021, p. 976 ; VÉLIZ, 2020, p. 74-75).

2.2.2.3. L'INTÉRÊT JURIDIQUE OU PRATIQUE IMPORTANT DÉFAVORABLEMENT AFFECTÉ PAR L'EXERCICE DU POUVOIR

[38] La Cour suprême a défini la notion d'intérêt juridique ou pratique important comme un « intérêt de droit privé précis sur lequel la personne exerçait déjà un droit distinct et absolu »[74]. Les intérêts humains fondamentaux et personnels ont aussi été reconnus comme des intérêts juridiques ou pratiques importants, mais l'incidence générale sur le « bien-être […] ou la sécurité d'une personne »[75] a été exclue de leur portée. L'évaluation de l'atteinte du critère est contextuelle. Selon nous, une interprétation libérale de la définition actuelle du critère pourrait servir à montrer que l'exercice du pouvoir par les plateformes peut défavorablement affecter des intérêts individuels

70 *Frame* c. *Smith*, préc., note 65, par. 63.

71 *Id.*

72 Voir par exemple : Commissariat à la protection de la vie privée du Canada, « Facebook refuse de remédier à des lacunes graves en matière de protection de la vie privée malgré s'être excusée publiquement d'avoir commis un « abus de confiance », communiqué, Ottawa, 25 avril 2019, en ligne : <https://www.priv.gc.ca/media/1807/consent_201605_f.pdf>.

73 Sur l'insuffisance des recours, voir Guevara (2021) : « Further, users do not have a remedy either in existing privacy laws, or in other areas of law such as tort and contract law. Existing privacy laws do not provide the user with an individual cause of action ». Le projet de loi fédéral C-27 pourrait en partie remédier aux problèmes de l'insuffisance des recours et du non-respect des conclusions du CPVP. Le projet de loi prévoit entre autres la mise en place d'un tribunal destiné à la protection des renseignements personnels et des données. Ce tribunal pourrait imposer, sur recommandation du CPVP, des sanctions administratives pécuniaires (voir notamment l'art. 94). Le projet de loi C-27, en instaurant la Loi sur la protection de la vie privée des consommateurs, crée aussi un nouveau droit privé d'action pour les individus (voir l'art. 107) et accorde de nouveaux pouvoirs d'ordonnance de conformité au CPVP (voir notamment l'art. 93).

74 *Alberta* c. *Elder Advocates of Alberta Society*, préc. note 64, par. 51.

75 *Id.*

importants qui devraient être pris en considération dans l'analyse. Toutefois, une redéfinition élargie du critère qui tient compte des intérêts de la collectivité serait plus adaptée au modèle d'affaires et au contexte d'exercice du pouvoir des plateformes en ligne.

▪ Des intérêts individuels affectés par l'exercice du pouvoir

[39] Les données personnelles peuvent servir aux entreprises dans le secteur du crédit à évaluer la solvabilité d'un individu. L'empreinte numérique d'une personne pourrait ainsi avoir un impact défavorable et discriminatoire sur sa capacité à obtenir un prêt (BIDDLE, 2019). Par exemple, l'application mobile *Lenddo* propose de calculer un pointage de crédit en mobilisant les données issues des activités sur les réseaux sociaux et sur les moteurs de recherche[76] (Autorité des marchés financiers, p. 23-24). Les pratiques des plateformes en ligne peuvent également avoir une incidence précise sur les émotions des personnes (KRAMER, 2014) et sur leur capacité à correctement s'informer (TRUDEL, 2021 ; BALKIN, 2022, p. 117-118 ; VÉLIZ, 2020 p. 80-81). Comme le rappelait le CPVP, « la vie privée est une condition préalable à l'exercice d'autres droits fondamentaux, notamment la liberté [et] l'égalité » (CPVP, 2019b). Les pratiques de collecte et de traitement des données par les plateformes sont ainsi à même de mettre en jeu des intérêts humains fondamentaux et personnels, mais aussi des droits individuels spécifiques.

▪ Une redéfinition du critère pour tenir compte des intérêts collectifs

[40] La perspective individualiste du critère d'intérêt juridique ou pratique important nous paraît inadaptée au contexte d'exercice du pouvoir par les plateformes. En effet, des atteintes inoffensives ou invisibles pour une personne peuvent entraîner des conséquences sociétales préjudiciables qui devraient être appréhendées par le droit à cette étape de l'analyse : « sometimes the only way to protect the individual is to protect the group to which the individual belongs. Preferably before any disaster happens. » (FLORIDI, 2014, p. 3) Le scandale de *Cambridge Analytica*, où la firme du même nom a subtilement ciblé des internautes pour influencer leur vote, en est un exemple (DETROW, 2018; GONZÁLEZ, 2017; VÉLIZ, 2020, p. 66-71). Le CPVP s'est d'ailleurs exprimé quant aux risques pour la société des pratiques d'influence du comportement et du microciblage, et ce, particulièrement lors de leur emploi dans le cadre d'une élection (CPVP, 2020). En 2014, Jonathan Zittrain écrivait que *Facebook* pourrait théoriquement décider de l'issue d'une élection sans que personne ne le réalise[77].

2.2.2.4. L'ENGAGEMENT DES PLATEFORMES À AGIR DANS LE MEILLEUR INTÉRÊT

[41] Via leurs politiques d'utilisation et de confidentialité, les plateformes incitent les internautes à leur faire confiance pour la protection de leurs données et de leur vie privée (GUEVARA, 2021). Cela milite en faveur de la reconnaissance d'un engagement

76 Lenddoefl Scoring, en ligne : < https://lenddoefl.com/scoring>

77 J. Zittrain, « Facebook could Decide an Election without Anyone Ever Finding Out », The New Statesman, 3 juin 2014, en ligne : <https://www.newstatesman.com/science-tech/2014/06/facebook-could-decide-election-without-anyone-ever-finding-out>.

implicite à agir dans leur meilleur intérêt[78]. Par exemple, sur le réseau social *Facebook*, il est possible de retrouver un engagement pour la protection des données[79], lequel indique que « Facebook prend la protection des données et la vie privée des personnes très au sérieux [et] qu'il s'engage à rester en accord avec les lois de protection des données »[80]. Cet engagement détaille également les efforts déployés par *Meta* en matière de protection de la vie privée et des données personnelles : renforcement de l'équipe de protection des données, embauche imminente d'un responsable de la protection des données et développement d'outils pour aider les personnes à gérer la confidentialité de leurs données et à « comprendre leurs choix concernant leurs données personnelles »[81]. En quelques clics, il est possible d'accéder à « l'Assistance confidentialité »[82] et au « Centre de confidentialité »[83]. La structure de cette dernière rubrique et le vocabulaire employé dans ses différentes sections donnent une impression de contrôle des membres sur leurs données personnelles et sur leur vie privée : « Protéger vos données permet de préserver votre confidentialité », « Contrôler qui peut voir ce que vous partagez sur Meta »[84]. Dans la section portant sur les publicités personnalisées, on retrouve l'indication suivante : « [n]ous attachons une grande importance à votre confidentialité, aussi bien dans notre manière de gérer vos informations que dans la transparence et le contrôle que nous vous fournissons »[85]. Les déclarations de *Facebook* rapportées par le CPVP dans le cadre de son enquête sur l'affaire *Cambridge Analytica* font aussi état de la volonté du réseau social à garantir à ses membres le respect de leur vie privée : « notre priorité est de garantir aux utilisateurs que la confiance qu'ils ont en Facebook est méritée et que [leurs] données sont protégées sur […] Facebook » (CPVP, 2019c, par. 169). Le critère de l'engagement à agir dans le meilleur intérêt ressort aussi des politiques de confidentialité de *Twitter* (« Nous traitons vos informations de manière équitable, quel que soit l'endroit du monde où vous vivez »[86]) et de façon encore plus évidente dans la politique de confidentialité de *Google* :

> Lorsque vous utilisez nos services, vous nous confiez vos données personnelles. Nous comprenons que c'est une grande responsabilité et nous faisons tout notre possible pour protéger vos renseignements et pour vous permettre de les gérer[87].

[42] Une interprétation libérale des quatre critères développés par la Cour suprême pour conclure à l'existence d'une relation fiduciaire *ad hoc* est une avenue plausible pour ouvrir la porte à la reconnaissance d'une telle relation entre les plateformes et leurs membres, et plus particulièrement pour donner lieu à l'imposition d'un devoir de loyauté.

78 *Galambos* c. *Perez*, préc., note 65, par. 79.

79 Meta, « L'engagement de Facebook pour la protection des données et la confidentialité, conformément au RGPD », 29 janvier 2018, en ligne : <https://www.facebook.com/business/news/facebooks-commitment-to-data-protection-and-privacy-in-compliance-with-the-gdpr>.

80 *Id.*

81 *Id.*

82 Meta, Assistance confidentialité Facebook, 2022, en ligne : <https://fr-ca.facebook.com/help/443357099 140264>.

83 Meta, Centre de confidentialité, 2022, en ligne : <https://www.facebook.com/privacy/center/?entry_ point=facebook_bookmarks>.

84 *Id.*, en ligne : <https://www.facebook.com/privacy/guide/adsv2>.

85 *Id.*, en ligne : <https://www.facebook.com/privacy/guide/adsv2>.

86 Twitter, Politique de confidentialité de Twitter, 2022, en ligne : <https://twitter.com/fr/privacy>.

87 Google, Politique de confidentialité et conditions d'utilisation, 2022, en ligne : <https://policies. google.com/privacy?hl=fr-CA>.

2.2.3. LE CONTENU DU DEVOIR FIDUCIAIRE DE LOYAUTÉ DES PLATEFORMES EN LIGNE

[43] En contexte numérique, le devoir de loyauté imposé aux plateformes pourrait s'ancrer dans l'objectif de garantir l'intérêt supérieur des utilisateurs et des utilisatrices dans le cadre de la relation de confiance qui s'établit entre eux et les plateformes (RICHARDS & HARTZOG, 2021, p. 995). L'intérêt supérieur découlerait de leurs attentes raisonnables relativement aux possibilités d'utilisation de leurs données par les plateformes, mais aussi relativement à la nature de leur expérience en ligne. Il s'agirait donc d'envisager le principe d'intérêt supérieur non pas comme l'atteinte d'une norme de bien-être abstraite, mais plutôt comme le fait de protéger les intérêts spécifiques associés au fait de confier ses données et son attention au réseau social (HARTZOG & RICHARDS, 2022, p. 1011-1012 et p. 1017-1019 ; LITMAN, 2006). Par exemple, la personnalisation loyale pourrait faire partie des attentes raisonnables des internautes en matière d'utilisation de leurs données personnelles. La publicité contextuelle pourrait donc être considérée comme une utilisation loyale des données, alors que la publicité comportementale irait à l'encontre de l'intérêt supérieur des internautes. Ainsi, une personne lisant un article sur un sujet en particulier pourrait raisonnablement s'attendre à recevoir de la publicité ciblée en lien avec ce sujet. Toutefois, ferait l'objet d'une pratique déloyale la personne qui serait confrontée à une publicité spécifique du fait du traitement de données issues de sources variées et ayant permis la découverte d'un nouveau savoir sur elle (BALKIN, 2020, p. 28 ; HARTZOG & RICHARDS, 2022, p. 1026-1027). Par ailleurs, l'influence loyale pourrait aussi faire partie des attentes raisonnables des internautes relativement à leur expérience en ligne sur les plateformes (HARTZOG & RICHARDS, 2022, p. 1029-1031). Si ces dernières ont recours à l'architecture des choix pour inciter les personnes à prendre une décision particulière dans l'environnement numérique, ce *design* n'est pas forcément déloyal. Utiliser des techniques issues des sciences comportementales pour s'assurer que les personnes prennent connaissance des conditions d'utilisation pourrait être perçu comme une pratique visant à favoriser l'intérêt supérieur des internautes[88]. Avoir recours aux *dark patterns*[89] ou à d'autres pratiques de *design* trompeur[90] en concevant, par exemple, une interface qui rend ardue pour les internautes la suppression de leur compte pourrait toutefois être considéré comme une pratique déloyale allant à l'encontre des attentes raisonnables en matière d'expérience en ligne.

2.2.4. LES AVANTAGES DE L'IMPOSITION D'UN DEVOIR FIDUCIAIRE DE LOYAUTÉ AUX PLATEFORMES EN LIGNE

▪ Une reconnaissance contextuelle

[44] D'abord, contrairement aux relations fiduciaires de fait (ex : médecin-patient), la reconnaissance d'une relation fiduciaire *ad hoc* est issue des circonstances factuelles spécifiques des relations plutôt que de la présence d'acteurs désignés. Le principe de la neutralité technologique est ainsi favorisé, en ce que la pérennité du modèle est

88 À ce sujet, Ryan Calo proposait en 2013 le concept de « visceral notice », où le design pourrait être conçu de manière à favoriser le consentement éclairé des personnes. Voir R. Calo, « Against Notice Skepticism in Privacy (and Elsewhere) », 2013, Notre Dame Law Review, V87, N3, p. 1038-1047.

89 Deceptive Design, What is Deceptive Design, en ligne : <https://www.deceptive.design/>.

90 Voir par exemple la typologie de la CNIL : « Une typologie non exhaustive de pratiques de design potentiellement trompeur » (CNIL, 2019, p. 29-30).

assurée face aux évolutions de la technologie et à la fluctuation des acteurs (CPVP, 2019b). Dans le même ordre d'idées, si des auteurs ont critiqué la possibilité d'imposer une obligation fiduciaire de loyauté aux plateformes en raison de sa nature trop vague, d'autres ont mis de l'avant qu'une telle norme pourrait s'éclaircir avec le temps, de façon analogue au concept de négligence, une notion vantée en droit pour sa flexibilité et sa capacité à s'adapter aux évolutions de la société (RICHARDS & HARTZOG, 2021, p. 1013). Ensuite, comme en fait état l'édition 2021 de *The Law of Trusts*, « fiduciary jurisprudence is one of the most confused and least understood areas of contempory law » (GILLEN & al, 2021, p. 682). La Cour suprême a en effet remanié le test visant à reconnaître les relations fiduciaires *ad hoc* à plusieurs reprises[91]. La codification de critères spécifiques dans la législation canadienne de protection des renseignements personnels assurerait ainsi la stabilité du droit, en plus de permettre l'ajustement des critères au contexte spécifique d'exercice du pouvoir des plateformes – en consacrant par exemple une interprétation collective du critère d'intérêt juridique ou pratique important examiné précédemment.

- Une protection en amont incombant aux plateformes

[45] L'imposition d'un devoir fiduciaire de loyauté via la codification d'un modèle fiduciaire dans la législation permettrait par ailleurs de garantir que les intérêts des utilisateurs et utilisatrices de plateformes soient respectés indépendamment de leur compréhension de l'environnement numérique, des conditions d'utilisation ou des politiques de confidentialité (RICHARDS & HARTZOG, 2021, p. 992). La vérification des risques liés au traitement des données et au *design* incomberait en effet aux entreprises qui collectent et traitent les données, et non aux internautes. Ce type de modèle aurait aussi l'avantage d'offrir une protection en amont qui n'exige pas la preuve de préjudice (HARTZOG & RICHARDS, 2022, p. 2020). Finalement, le devoir de loyauté permettrait de circonscrire l'innovation dans des limites socialement acceptables. Un parallèle peut ici être fait avec les normes environnementales, qui posent des limites à la maximisation des profits des entreprises en réglementant l'utilisation qu'elles peuvent faire des ressources (BALKIN, 2020, p. 23).

2.2.5. LES DIFFICULTÉS DE L'IMPOSITION D'UN DEVOIR FIDUCIAIRE DE LOYAUTÉ AUX PLATEFORMES EN LIGNE

[46] La mise en œuvre d'un modèle fiduciaire pose toutefois des difficultés. La manipulation des internautes est actuellement « baked into the business model » (BALKIN, 2020, p. 26). Assujettir les plateformes à un devoir de loyauté impliquerait pour elles de changer du tout au tout leurs pratiques commerciales actuelles, des changements qui ne s'imposeraient pas sans résistance[92] (KELLER, 2021, p. 236). Des obstacles liés à la mise en application pratique d'une telle obligation, semblables à ceux soulevés pour les fiducies de données, se posent aussi : comment surveiller les entreprises pour s'assurer qu'elles respectent leurs obligations ? Comment vérifier quelles données ont été utilisées pour s'assurer de l'absence de personnalisation

91 *Frame* c. *Smith*, (1987); *Lac Minerals Ltd.* c. *International Corona Resources Ltd.*; *Hodgkinson* c. *Simms*; *Galambos* c. *Perez*; *Alberta* c. *Elder Advocates of Alberta Society*, préc., note 65.

92 Reuters, « Google U.S. lobbying jumps 27% as lawmakers aim to rein in Big Tech », 20 janvier 2022, en ligne : <https://www.reuters.com/technology/google-us-lobbying-jumps-27-lawmakers-aim-rein-big-tech-2022-01-20/>.

déloyale ? Comment concrètement distinguer la personnalisation de la manipulation ? Finalement, et malgré les explications fournies par certains auteurs (BALKIN, 2020, p. 23-24; HARTZOG et RICHARDS, 2022, p. 1010), il est difficile de concevoir comment, en pratique, les plateformes pourraient à la fois prétendre maximiser les intérêts de leurs actionnaires et ceux, opposés, de leurs membres (DELACROIX & LAWRENCE, 2019, p. 241; KHAN & POZEN, 2019, p. 504-506).

CONCLUSION

[47] Aujourd'hui plus que jamais, les données sont des informations relationnelles et chaque action – ou omission – d'une personne dans l'environnement numérique a des conséquences sur les autres. Dès lors, les lois de protection des renseignements personnels, en appréhendant erronément la vie privée comme une question de nature essentiellement individuelle et en faisant abstraction des asymétries de pouvoir et d'information en présence, peinent à protéger les personnes. Il apparaît donc nécessaire de réfléchir à de nouveaux modes de réglementation. Dans le contexte des plateformes en ligne, les fiducies de données et le devoir fiduciaire de loyauté sont des avenues intéressantes, mais lacunaires. La mise en œuvre des fiducies de données est compromise par un manque d'incitatifs pour attirer des fiduciaires, par la méfiance des personnes à confier leurs données personnelles à un acteur externe, par la difficulté de surveillance effective du comportement des fiduciaires et par la quasi-impossibilité de retrouver un contrôle sur des millions de données déjà collectées, traitées et inférées. Si constituées, les fiducies de données seraient aussi à même de reproduire les carences du modèle de *notice and choice* et de faire renaître une asymétrie de pouvoir entre fiduciaires et internautes. De son côté, le devoir de loyauté, s'il présente l'avantage d'envisager la vie privée dans une perspective relationnelle, serait toutefois difficile à mettre en œuvre : il ébranlerait les bases mêmes des pratiques commerciales actuelles des plateformes, soulèverait un conflit entre les intérêts de ces dernières et ceux des internautes, et poserait des difficultés quant aux mécanismes de surveillance pouvant être mis en place. Le droit à la vie privée, tant dans sa conception individuelle que collective, ne suffit pas à protéger les personnes. L'apport d'autres branches du droit, comme le droit de la consommation et de la concurrence, est nécessaire (RICHARDS & HARTZOG, 2021, p. 1020). La rééquilibration des relations de pouvoir via la limitation du monopole des géants du numérique, par exemple, pourrait favoriser la concurrence légitime et contribuer à offrir un véritable choix aux internautes (MAZZUCATO, 2018).

RÉFÉRENCES BIBLIOGRAPHIQUES

Législation

Législation fédérale

Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois, projet de loi nº C-27 (dépôt et 1re lecture – 16 juin 2022), 1re sess., 44e légis. (Can.)

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, c. 5

Législation provinciale

Code civil du Québec, RLRQ, c CCQ-1991

Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, projet de loi nº 64, L.Q. 2021, c. 25

Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ, c. P-39.1

Jurisprudence

Alberta c. Elder Advocates of Alberta Society, 2011 CSC 24

Can. Aero c. O'Malley, (1974) R.C.S. 592

Douez c. Facebook Inc., 2017 CSC 33

Douez c. Facebook Inc., 2022 BCSC 914

Frame c. Smith, (1987) 2 R.C.S. 99

Galambos c. Perez, 2009 CSC 48

Hodgkinson c. Simms, (1994) 3 R.C.S. 377

Lac Minerals Ltd. c. International Corona Resources Ltd., (1989) 2 R.C.S. 574

McInerney c. MacDonald, (1992) 2 R.C.S. 138

Norberg c. Wynrib, (1992) 2 R.C.S. 226

Option Consommateurs c. Google, 2022 QCCS 2308

R. c. Dyment, (1988) 2 R.C.S. 417

Royal Trust Co. c. Tucker, (1982) 1 R.C.S. 250

Strother c. 3464920 Canada Inc., 2007 CSC 24

Doctrine

Monographies, ouvrages collectifs et rapports

Ada LOVELACE INSTITUTE ET UK AI COUNCIL, *Exploring legal mechanisms for data stewardship*, 2021, en ligne, <https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/>

AUTORITÉ DES MARCHÉS FINANCIERS, *L'intelligence artificielle en finance. Recommandations pour une utilisation responsable*, novembre 2021, en ligne : <https://lautorite.qc.ca/grand-public/publications/pour-les-professionnels>

BALKIN, J. M., « To Reform Social Media, Reform Informational Capitalism », dans L. Bollinger and G. R. Stone (dir.), *Social Media, Freedom of Speech and the Future of Our Democracy*, Oxford, Oxford University Press, 2022

BENYEKHLEF, K. et P. L. DÉZIEL, *Le droit à la vie privée en droit québécois et canadie*n, Cowansville, Éditions Yvon Blais, 2018

BENYEKHLEF, K., « Les glissements du droit à la vie privée. De Feydeau à Facebook : de la comédie de mœurs à l'économie des données », V. Gautrais, C. Régis et L. Largenté (dir.), *Mélanges Patrick Molinari*, Montréal, Éditions Thémis, 2018

BPE SOLICITORS, PINSENT MASONS et C. REED, *Data trusts: legal and governance considerations*, avril 2019, en ligne : <https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf>

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Consentement et protection de la vie privée. Document de discussion sur les améliorations possibles au consentement sous le régime de la Loi sur la protection des renseignements personnels et les documents électroniques*, Ottawa, 2016, en ligne : <https://www.priv.gc.ca/media/1807/consent_201605_f.pdf>

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée de 2020-2021. Rapport final*, Ottawa, 2021, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2021/por_2020-21_ca/>

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Un cadre réglementaire pour l'IA : recommandations pour la réforme de la LPRPDE,* Consultation sur l'intelligence artificielle, Ottawa, 2020, en ligne : <https://www.priv.gc.ca/fr/a-propos-

du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-ai/reg-fw_202011/>

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Facebook refuse de remédier à des lacunes graves en matière de protection de la vie privée malgré s'être excusée publiquement d'avoir commis un « abus de confiance », communiqué, Ottawa, 25 avril 2019a, en ligne : <https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2019/nr-c_190425/>

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Réforme des lois sur la vie privée : Pour faire respecter les droits et rétablir la confiance envers le gouvernement et l'économie numérique*, Ottawa, 2019b, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/201819/ar_201819/>

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Enquête conjointe du Commissariat à la protection de la vie privée du Canada et du Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique au sujet de Facebook, Inc.*, Ottawa, 2019c, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2019/lprpde-2019-002/>

COMMISSION DE RÉFLEXION ET DE PROPOSITIONS SUR LE DROIT ET LES LIBERTÉS À L'ÂGE NUMÉRIQUE, *Numérique et libertés : Un nouvel âge démocratique*, France, Rapport nº 3119, XIVe Législature, 2015, en ligne : <https://www.assemblee-nationale.fr/14/pdf/rapports/r3119. pdf>

DE SAINT PULGENT, M., « Les besoins d'interrégulation engendrés par Internet. Propos Introductifs », dans M.-A. FRISON-ROCHE (dir.), *Internet, espace d'interrégulation*, Paris, Dalloz, 2016

DENHAM, E., *Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques*, Commissariat à la protection de la vie privée du Canada, Ottawa, 2009, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2009/lprpde-2009-008/>

ELEMENT AI ET NESTA, *Fiducies de Données. Un nouvel outil pour la gouvernance des données*, 2019, en ligne : <https://hello.elementai.com/rs/024-OAQ-547/images/Fiducies_de_Donnees_ FR_201914.pdf>

ELLIS, M. V., *Corporate & Commercial Fiduciary Duties*, Toronto, Carswell, 1995

GAUTRAIS, V. et P. TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Montréal, Éditions Thémis, 2010

GILLEN, M. R., F. WOODMAN, J. B. BERRYMAN, D. FREEMAN, P. GIRARD, M. P. HARRINGTON, D. MACPHERSON, K. McNEIL, M. J. MOSSMAN et J. PHILLIPS, *The Law of Trusts. A Contextual Approach*, Toronto, Emond Montgomery Publications Limited, 2021

GOUVERNEMENT DU CANADA, INNOVATION, SCIENCES ET DÉVELOPPEMENT ÉCONOMIQUE CANADA, *Renforcer la protection de la vie privée dans l'ère numérique. Propositions pour moderniser la Loi sur la protection des renseignements personnels et des documents électroniques*, Ottawa, 2019, en ligne : <https://ised-isde.canada.ca/site/innover-meilleur-canada/fr/charte-canadienne-numerique/renforcer-protection-vie-privee-dans-lere-numerique>

GRAEF, I., *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility*, Alphen aan den Rijn, Wolters Kluwer, 2016

GROUPE D'EXAMEN DU CADRE LÉGISLATIF EN MATIÈRE DE RADIODIFFUSION ET DE TÉLÉCOMMUNICATION, *L'avenir des communications au Canada : le temps d'agir : rapport final / Examen du cadre législatif en matière de radiodiffusion et de télécommunications*, Ottawa, 2020

LEBLANC, J., *Definition and Implementation of Data Trusts in Quebec Civil Law*, Territoires innovants en économie sociale et solidaire (TIESS), Montréal, 2021, en ligne : <https://tiess.ca/wp-content/uploads/2021/03/Data-Trusts-In-Quebec-Civil-Law-Synthesis-2.pdf>

LECHEVALIER, F., *Les fiducies de données personnelles de santé : étude illustrée des enjeux et bénéfices d'une gestion collective de la propriété des données personnelles de santé*, mémoire de maîtrise et Master, Québec (Canada) et Cachan (France), Facultés de droit, Université Laval et Université Paris-Saclay, 2020

MOZILLA INSIGHTS, J. van GEUNS et A. BRANDUSESCU, *Shifting Power Through Data Governance*, 2020, en ligne : <https://assets.mofoprod.net/network/documents/ShiftingPower.pdf>

PRIVACY INTERNATIONAL, H*ow Apps on Android Share Data with Facebook (even if you don't have a Facebook account*, décembre 2018, en ligne : < https://privacyinternational.org/report/2647/how-apps-android-share-data-facebook-report>

ROCHFELD, J. « Contre l'hypothèse de la qualification des données personnelles comme des biens », dans E. NETTER et A. CHAIGNEAU (dir.), *Les biens numériques*, CEPRISCA, Collection Colloques, 2015, p. 221-236

SCHMIDT, D. C., *Google Data Collection*, Digital Content Next, 2018, en ligne : <https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf>

THALER R. H. et C. R. SUNSTEIN, *Nudge: Improving decisions about health, wealth, and happiness*, Londres, Yale University Press, 2008

TRUDEL P., « Fausses nouvelles et réseaux sociaux », dans M. STANTON-JEAN et C. HERVÉ (dir.), *Éthique, intégrité scientifique et fausses nouvelles*, Paris, Dalloz, 2021

WESTIN, A., *Privacy and Freedom*, New York, Atheneum, 1967

VAAST, A., *La patrimonalisation des données personnelles*, Éditions L'Harmattan, Collection INTER-NATIONAL, Série Premières Synthèses, 2021

VAN ERP, S., « Management as Ownership of Data », dans S. Lohsse, R. Schulze et D. Staudenmayer (dir.), *Data as counter-performance - contract law 2.0? : Münster Colloquia on EU Law and the Digital Economy V*, Nomos, 2020

VÉLIZ, C., *Privacy Is Power: Why and How You Should Take Back Control of Your Data*, Londres, Bantam Press, 2020

ZUBOFF, S., *The Age of Surveillance Capitalism*, New York, PublicAffairs, 2019

Articles de revues

ALLEN, A. L., « Protecting One's Own Privacy in a Big Data Economy », 2016, Harvard Law Review Forum, V130, N171, p. 71-78

BALKIN, J. M., « The Fiduciary Model of Privacy », 2020, Harvard Law Review Forum, V134, N1, p. 11-33

BEN-SHAHAR, O., « Data Pollution », 2019, Journal of Legal Analysis, V11, N1, p. 104-159

BIRCH, K., DT COCHRANE et C. WARD, « Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech », 2021, Big Data & Society, V8, N1, p. 1-15

BORDEN LADNER GERVAIS, *Canada's Consumer Privacy Protection Act (Bill C-27): Impact for businesses*, juin 2021, en ligne : <https://www.blg.com/en/insights/2022/06/canadas-consumer-privacy-protection-act-bill-c27-impact-for-businesses>

BOURCIER, D. et De FILIPPI, P., « Vers un droit collectif sur les données de santé », 2018, *Revue de droit sanitaire et social*, N3, p. 444-456

CALO, R., « Against Notice Skepticism in Privacy (and Elsewhere) », 2013, *Notre Dame Law Review*, V87, N3, p. 1027-1072

DELACROIX, S. et LAWRENCE, N. D., « Bottom-up *data Trusts*: disturbing the 'one size fits all' approach to data governance », 2019, *International Data Privacy Law*, V9, N4, p. 236-252

DÉZIEL, P.-L., « Les limites du droit à la vie privée à l'ère de l'intelligence artificielle : groupes algorithmiques, contrôle individuel et cycle de traitement de l'information », 2018, *Les Cahiers de propriété intellectuelle*, V30, N3, p. 827-847

DÉZIEL, P.-L., « La valorisation des renseignements personnels au Québec et au Canada : la promesse des projets de loi no 64 et C-11 », 2021, *Les Cahiers de propriété intellectuelle*, V33, N2, p. 1193-1240

DU PERRON, S., « La vie privée des groupes : nouveau cadre théorique pour une protection contre le profilage algorithmique », dans L. R. Zannou et E. Gaumond, (dir.), *Vulnérabilité(s) : L'appréhension des défis du numérique par le droit*, Montréal, Lex Electronica, N25, V2, 2020, p. 36-47, en ligne : <http://lexelectronica.openum.ca/s/1959%20Available%20at:%20>

EDWARDS, L., « Reconstructing consumer privacy protection on-line: a modest proposal », 2004, *International Review of Law, Computers & Technology*, V18, N3, p. 313-344

FAIRFIELD, J. A. T. et C. ENGEL, « Privacy as a Public Good », 2015, *Duke Law Journal*, V65, N3, p. 385-457

FLORIDI, L., « Open Data, Data Protection, and Group Privacy », 2014, *Philosophy & Technology*, V27, N1, p. 1-3

GRENON, A., « La fiducie canadienne issue de la common law : le droit comparé peut-il favoriser son évolution? », 2006, *Revue de droit d'Ottawa*, V40, p. 83-100

GONZÁLEZ, R. J., « Hacking the citizenry? Personality profiling, "big data" and the election of Donald Trump », 2017, *Anthropology Today*, V3, N3, p. 9-12

HARTZOG, W. et N. RICHARDS, « The Surprising Virtues of Data Loyalty », 2022, *Emory law journal*, V71, N5, p. 985-1033

HOUSER, K. et J. W. BAGBY, « The Data Trust Solution to Data Sharing Problems », à paraître 2022, V*anderbilt Journal of Entertainment & Technology Law*

KHAN, L. M. et D. E. POZEN, « A Skeptical View of Information Fiduciaries », 2019, *Harvard Law Review*, V133, N2, p. 497-541

KELLER, D., « Amplification and its discontents: Why regulating the reach of online content is hard », 2021, V1, N1, p. 227-272

KRAMER, A. D. I., J. E. GUILLORY et J. T. HANCOCK, « Experimental evidence of massive-scale emotional contagion through social networks », 2014, *Proceedings of the National Academy of Sciences of the United States of America*, V111, N24, p. 8788-8790

KRÖGER, J. L., M. MICELI et F. MÜLLER, « How Data Can Be Used Against People: A Classification of Personal Data Misuses », 2021, *SSRN Electronic Journal*

LAIDLAW, E., « Mapping Current and Emerging Models of Intermediary Liability », 2019, *SSRN Electronic Journal*

LAZARO, C. et D. LE MÉTAYER, « Le consentement au traitement des données personnelles. Perspective comparative sur l'autonomie du sujet », 2014, *Revue juridique Themis*, V48, N3, p. 765-815

MARINOTTI, J., « Data Types, Data Doubts & *Data Trusts* », à paraître 2022, *New York University Law Review Online*

McDONALD A. M. et L. F. CRANOR, « The Cost of Reading Privacy Policies », 2008, *I/S: A Journal of Law and Policy for the Information Society*, V4, N3, P. 540-565

MOURON, P., « Pour ou contre la patrimonialité des données personnelles », 2018, *Revue européenne des médias et du numérique*, p. 90-96

NORMAND, S., « Les nouveaux biens », 2004, *Revue du notariat*, V106, N2, p. 177-204

O'HARA, K., « Data Trusts », 2020, *European Data Protection Law Review*, V6, N4, p. 484-491

PICCINI ROY, M., « Trusts in Quebec », dans Trusts in prime jurisdictions, Londres, *Globe Law and Business*, 2010, p. 343-362

PLOUG T et S. HOLM, « Meta consent: A flexible and autonomous way of obtaining informed consent for secondary research », 2015, *BMJ*, V350, en ligne : <https://doi.org/10.1136/bmj.h2146>

POULLET, Y., « Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle », 2021, *Revue des affaires européennes*, N1, p. 87-101

RICHARDS, N. et W. HARTZOG, « A Duty of Loyalty for Privacy Law », 2021, *Washington University Law Review*, V99, N3, p. 961-1021

RICHARDS, N. et W. HARTZOG, « The Pathologies of Digital Consent », 2019, *Washington University Law Review*, V96, N6, p. 1461-1503

RINIK, C., « Data trusts: more data than trust? The perspective of the data subject in the face of a growing problem », 2020, *International Review of Law*, Computers & Technology, V4, N3, p. 342-363

SAETRA, H. S., « Privacy as an aggregate public good », 2020, *Technology in Society*, V63, p. 1-9

SAVAGE, C. W., « Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy », 2019, *Standford Law Review*, V22, N1 p. 95-162

SCOTT, A. W., « The Fiduciary Principle », 1949, *California Law Review*, V37, N4, p. 539-555

SOLOVE, D. J., « Introduction: Privacy Self-Management and the Consent Dilemma », 2012, *Harvard Law Review*, V 126, N 7, p. 1880-1903

SOLOVE, D. J., « The Myth of the Privacy Paradox », 2020, The George *Washington Law Review*, V89, N1, p. 1-51

STOEKLÉ, H.-C., J.-F. DELEUZE, G. VOGT et C. HERVÉ, « Vers un consentement éclairé dynamique », 2017, *Médecine/Sciences*, V3, N2, p. 188-192

SWIRE, P., « Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment », 2012, *North Carolina Law Review*, V 90, N5, p. 1371-1416

WARNER, R., « Notice and Choice Must Go: The Collective Control Alternative », 2020, *Science and Technology Law Review*, V23, N2, p. 172-195

Billets de blogues et articles de journaux

BARBEAU, B., « Les données de la RAMQ pour appâter les pharmaceutiques », Radio-Canada Info, 21 août 2020, en ligne : <https://ici.radio-canada.ca/nouvelle/1728106/pierre-fitzgibbon-compagnies-pharmaceutiques-donnes-medicales-mila>

BIDDLE, S., « Thanks to Facebook, Your Cellphone Company Is Watching You More Closely Than Ever », *The Intercept*, 20 mai 2019, en ligne : <https://theintercept.com/2019/05/20/facebook-data-phone-carriers-ads-credit-score/>

DEGLISE, F., « Ottawa dit non à Mila et son application COVI de recherche de contacts de personnes contaminées », *Le Devoir*, 10 juin 2020, en ligne : <https://www.ledevoir.com/societe/580507/ottawa-dit-non-a-mila>

DETROW, S., « What Did Cambridge Analytica Do During The 2016 Election? », *National Public Radio*, 20 mars 2018, en ligne : <https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election>

GRAMMOND, S., « Desjardins, Capital One, TransUnion, et après? », *La Presse*, 17 octobre 2019, en ligne : <https://www.lapresse.ca/elections-federales/2019-10-17/desjardins-capital-one-transunion-et-apres>

HULIN, A.-S., « Introduction à la fiducie québécoise de données », *Territoires innovants en économie sociale et solidaire*, 15 décembre 2020, en ligne : <https://cyberjustice.openum.ca/ 2020/11/26/introduction-a-la-fiducie-quebecoise-de-donnees/>

HULIN, A.-S. et A. COSSÉ, « Pour une fiducie de données à la RAMQ », *Le Devoir*, 1er septembre 2020, en ligne : <https://www.ledevoir.com/opinion/idees/585113/pour-une-fiducie-de-donnees-a-la-ramq>

JUNG, D., « COVID-19 : l'application de traçage du Mila mise au placard par Ottawa », *Radio-Canada Info*, 10 juin 2020, en ligne : <https://ici.radio-canada.ca/nouvelle/1710961/ coronavirus-tracage-application-mila-canada>

LAWRENCE, N., « Data trusts could allay our privacy fears », The Guardian, 3 juin 2016, en ligne : <https://www.theguardian.com/media-network/2016/jun/03/data-trusts-privacy-fears-feudalism-democracy>

OPEN DATA INSTITUTE, « Defining a 'data trust' », *Open Data Trust*, 19 octobre 2018, en ligne : <https://theodi.org/article/defining-a-data-trust/>

MAZZUCATO, M., « Let's make private data into a public good », *MIT Technology Review*, 27 janvier 2018, en ligne : <https://www.technologyreview.com/2018/06/27/141776/lets-make-private-data-into-a-public-good/>

REUTERS, « Google U.S. lobbying jumps 27% as lawmakers aim to rein in Big Tech », 20 janvier 2022, en ligne : <https://www.reuters.com/technology/google-us-lobbying-jumps-27-lawmakers-aim-rein-big-tech-2022-01-20/>.

TRUDEL, P. « La valeur de nos données personnelles », *Le Devoir*, 13 mars 2018, en ligne : <https://www.ledevoir.com/opinion/chroniques/522496/la-valeur-de-nos-donnees-personnelles>

VÉLIZ, C., « Privacy is a collective concern », *The New Statesman*, 22 octobre 2019, en ligne : <https://www.newstatesman.com/science-tech/2019/10/privacy-collective-concern>

WYLIE, B. et S. M. McDONALD, « What Is a Data Trust? », *Center for International Governance Innovation*, 9 octobre 2018, en ligne : <https://www.cigionline.org/articles/what-data-trust/>

ZITTRAIN, J., « Facebook could decide an election without anyone ever finding out », *The New Statesman*, 3 juin 2014, en ligne : <https://www.newstatesman.com/science-tech/2014/06/ facebook-could-decide-election-without-anyone-ever-finding-out>

Autres références électroniques

ALSDURF, H., E. BELLIVEAU, Y. BENGIO, T. DELEU, P. GUPTA, D. IPPOLITI, R. JANDA, M. JARVIE, T. KOLODY, S. KRASTEV, T. MAHARAJ, R. OBRYK, D. PILAT, V. PISANO, B. PRUD'HOMME, M. QU, N. RAHAMAN, I. RISH, J.-F. ROUSSEAU, V. SCHMIDT, A. SHARMA, B. STRUCK, J. TANG, M. WEISS et Y. W. YU, « COVI White Paper - Version 1.0 », 2020, en ligne : <https://arxiv.org/abs/ 2005.08502>

DECEPTIVE DESIGN, *What is Deceptive Design*, en ligne : <https://www.deceptive.design/>

GOOGLE, P*olitique de confidentialité et conditions d'utilisation*, 2022, en ligne : <https://policies. google.com/privacy?hl=fr-CA>

GUEVARA, I., « Data Fiduciaries and Privacy Protection in the Digital Age », *Association du Barreau canadien*, 27 août 2021, en ligne : < https://www.cba.org/Sections/Privacy-and-Access/Resources/Resources/2021/PrivacyEssayWinner2021>

LEBLANC, J., *Conference Report. Data Trusts in Quebec's Civil Law Tradition. Webinar held on December 3, 2020, by Jessica Leblanc, TIESS.*, 2020, en ligne : <https://www.passerelles. quebec/system/files/upload/documents/posts/2020.12.11_conference_report_data_trust_jl.pd>

LENDDO, *Scoring*, en ligne : < https://lenddoefl.com/scoring>

LITMAN, M. m., « Droit de l'obligation fiduciaire », *Encycopédie canadienne*, 7 février 2006, en ligne : <https://www.thecanadianencyclopedia.ca/fr/article/obligation-fiduciaire-loi-sur-l>

META, « À propos des publicités sur Facebook », 2022, en ligne : <https://www.facebook.com/ ads/about/?entry_product=ad_preferences_hub>

META, *Assistance confidentialité Facebook*, 2022, en ligne : <https://fr-ca.facebook.com/help/ 443357099140264>

META, *Centre de confidentialité*, 2022, en ligne : <https://www.facebook.com/privacy/center/ ?entry_point=facebook_bookmarks>

META, *Conditions de service*, en ligne : <https://www.facebook.com/legal/terms/update>

META, Facebook*. Avec Facebook, partagez et restez en contact avec votre entourage*, 2022, en ligne : <https://www.facebook.com/>

META, « L'engagement de Facebook pour la protection des données et la confidentialité, conformément au RGPD », 29 janvier 2018, en ligne : <https://www.facebook.com/ business/news/facebooks-commitment-to-data-protection-and-privacy-in-compliance-with-the-gdpr>

META, *Politique de confidentialité*, en ligne : <https://www.facebook.com/privacy/policy/?entry_ point=data_policy_redirect&entry=0>

META, *Politique d'utilisation des cookies*, en ligne : <https://www.facebook.com/policies/ cookies/>

TWITTER, *Politique de confidentialité de Twitter*, 2022, en ligne : <https://twitter.com/fr/privacy>

Autres publications d'organisations publiques

ACADÉMIE DE LA TRANSFORMATION NUMÉRIQUE, *Portrait numérique des générations*, 2022, en ligne : <https://transformation-numerique.ulaval.ca/enquetes-et-mesures/netendances/2022-07-portrait-numerique-des-generations>

BORDEN LADNER GERVAIS, *Comparison of the proposed Consumer Privacy Protection Act ("CCPA") under C-11 (2020) and C-27 (2022)*, juin 2021 en ligne : <https://www.blg. com/en/insights/2022/06/canadas-consumer-privacy-protection-act-bill-c27-impact-for-businesses>

COMMISSION DE L'INFORMATIQUE ET DES LIBERTÉS, « La forme des choix : Données personnelles, *design* et frictions désirables », 2019, *Cahiers IP*, N6, p. 1-49

COMMISSION DE L'INFORMATIQUE ET DES LIBERTÉS, « Vie privée à l'horizon 2020. Parole d'experts », 2012, *Cahiers IP*, N1, p. 1-60

DÉZIEL, P.L., K. BENYEKHLEF et E. GAUMOND, *Repenser la protection des renseignements personnels à la lumière des défis soulevés par l'IA*, Document de réponse aux questions posées par la Commission d'accès à l'information du Québec dans le cadre de la consultation sur l'intelligence artificielle, OBVIA et Laboratoire de cyberjustice, 2020, en ligne : <http://collections.banq.qc.ca/ark:/52327/bs4067010>v