*Vol. 30, n° 3*

# 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

**Pierre-Luc Déziel***

RÉSUMÉ . . . . . 829

INTRODUCTION . . . . . 831

1. LA PRÉDICTION DES ATTRIBUTS PERSONNELS : LES PERSONNES COMME CIBLES. . . . . 831

   1.1 Target et l'anecdote de la jeune femme enceinte. . . . . 832

   1.2 Que disent les données lorsque l'intelligence artificielle les fait parler ? . . . . . 833

2. LES LIMITES DE LA PROTECTION JURIDIQUE DES PERSONNES ET DES RENSEIGNEMENTS PERSONNELS . . . . . 837

   2.1 La limite ontologique : la protection des groupes algorithmiques . . . . . 838

   2.2 La limite opérationnelle : le contrôle sur les renseignements et le principe du consentement individuel. . . . . 841



* Professeur adjoint à la Faculté de droit de l'Université Laval.]

[Note : cet article a été soumis à une évaluation à double anonymat.]

2.3 La limite structurelle : le cycle de traitement de l'information . . . . . 844

CONCLUSION . . . . . 846

**RÉSUMÉ**

Nos données personnelles sont collectées sans que nous en soyons toujours conscients. Cet article vise, par conséquent, à éclaircir le processus par lequel l'intelligence artificielle parvient à compiler de telles informations et à démontrer pourquoi la législation canadienne ne peut prétendre à protéger la vie privée dans une telle situation.

**MOTS-CLÉS**

accès à l'information (données personnelles) ; droit de la personne (données personnelles ; vie privée) ; banques de données ; intelligence artificielle ; Internet (données personnelles) ; vie privée (publicités pertinentes [ciblées])

## INTRODUCTION

Les techniques de traitement algorithmique de l'information engendrent la création d'un savoir sur les personnes qui menace leur vie privée. Par l'analyse de données primaires, certaines techniques d'intelligence artificielle permettent la découverte de traits personnels et d'habitudes de vie que les personnes peuvent raisonnablement s'attendre à garder privés. Cet article poursuit deux séries d'objectifs. Dans un premier temps, il s'agit de décrire comment cette connaissance est créée, de préciser ce qu'elle peut révéler et d'illustrer comment elle peut être utilisée pour agir sur le comportement des personnes. Dans un second temps, il s'agit d'expliquer pourquoi les lois canadiennes de protection des renseignements personnels ne peuvent que difficilement prétendre à une protection adéquate des personnes à l'ère de l'intelligence artificielle. Trois limites seront soumises à l'examen : une limite ontologique, portant sur les types d'entités qu'ignore le droit ; une limite opérationnelle, qui porte sur la notion de contrôle individuel et sur le principe du consentement ; et une limite structurelle, qui porte sur le cycle de traitement de l'information qui structure la suite d'obligations imposées aux entités qui assurent la gestion des renseignements personnels.

## 1. LA PRÉDICTION DES ATTRIBUTS PERSONNELS : LES PERSONNES COMME CIBLES

Dans cette première partie, je tenterai d'expliquer comment certaines techniques d'intelligence artificielle permettent la création d'un savoir sur les personnes qui peut être mobilisé pour agir sur leurs comportements. Pour ce faire, je débuterai par une anecdote qui illustre certains des enjeux que soulève le traitement algorithmique de l'information (1.1). Ensuite, je passerai en revue certains travaux récents qui portent sur la prédiction d'attributs personnels au moyen de techniques d'apprentissage automatique et d'apprentissage profond (1.2).

### 1.1 Target et l'anecdote de la jeune femme enceinte

L'anecdote de la jeune femme enceinte fut initialement rapportée par Charles Duhigg, journaliste au *New York Times*, dans un article qui s'intéresse aux secrets que détiennent les compagnies au sujet de leurs clients[1]. En 2011, un homme entre dans une succursale de la chaîne de magasins Target située en bordure de Minneapolis, au Minnesota, et demande à parler au gérant. L'homme est en colère. Il se demande pourquoi la compagnie envoie à sa jeune fille des coupons-rabais pour des articles de bébés alors que celle-ci est encore à l'école secondaire. Il clame que cette publicité peut l'inciter à tomber enceinte. Le gérant, surpris, ne sait pas quoi répondre et s'excuse. Quelques jours plus tard, le gérant rappelle le père, encore pour s'excuser, mais c'est plutôt celui-ci qui lui demande pardon. Après être rentré à la maison, le père eut une discussion avec sa fille. La vérité est que Target n'incitait pas la jeune femme à tomber enceinte ; Target avait en réalité compris qu'elle était enceinte et voulait lui soumettre une offre publicitaire personnalisée. La jeune femme n'avait pas dit à son père qu'elle attendait un enfant, pas plus qu'elle n'en avait informé Target. Mais la compagnie avait réussi, elle, à « deviner » ce fait intime.

Cette courte anecdote soulève deux questions importantes : pourquoi est-ce que Target s'intéresse aux femmes enceintes ? Et comment est-ce que la compagnie fait pour établir que certaines de ses clientes sont enceintes ? Comme l'explique Duhigg, les habitudes de consommation des personnes sont normalement fixées par une routine bien établie. On achète de la nourriture à l'épicerie, des médicaments à la pharmacie, des vêtements dans les boutiques, mais on ne se rend chez Target que pour se procurer certains items précis, comme des sous-vêtements à bas prix ou des produits nettoyants. Mais Target vend aussi de la nourriture, des médicaments et des vêtements, et la compagnie voudrait que ses clients fassent l'ensemble de leurs achats dans ses succursales. Comment réorienter le client ? Comment changer sa routine ? La solution de Target, qui est tout aussi brillante qu'inquiétante, est d'attendre que la vie d'une personne change subitement et entraîne un chamboulement de ses habitudes de vie et de consommation. La plasticité du comportement de cette personne offre de nouvelles perspectives à la compagnie, qui peut alors agir de manière à la réorienter vers ses succursales et ses produits. Pour Target, un de ces moments pivots où les habitudes d'une personne sont susceptibles de changer est l'arrivée d'un nouveau-né.

---

1. Charles DUHIGG, « How Companies Learn Your Secrets », *The New York Times*, 12 février 2012, en ligne : <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp>.

Si la compagnie était en mesure d'identifier les femmes enceintes, elle pourrait adapter sa publicité. Pour ce faire, Target se tourne alors vers une denrée précieuse et aujourd'hui encore mal protégée par le droit : les renseignements personnels. Par le biais de techniques de traitement de l'information, Target réussit à prédire, avec un certain degré de certitude, les probabilités qu'une de ses clientes soit enceinte. Chaque cliente de Target est assignée à un identifiant unique auquel correspond un dossier répertoriant l'ensemble des achats passés et comprenant des renseignements démographiques. Certains de ces renseignements sont collectés par Target directement auprès de ses clientes, alors que d'autres sont achetés à des tiers ou glanés dans des registres publics. Il fut possible pour Target d'identifier les clientes qui avaient des enfants, de déterminer à quel moment elles avaient accouché et de retracer l'historique d'achats de ces clientes pour les mois qui avaient précédé le jour de la naissance. En comparant ces historiques d'achats, des motifs se répétèrent, des tendances s'établirent et des patterns émergèrent. Target réussit à identifier 25 produits – comme des lotions ou des suppléments de zinc ou de magnésium – qui, ensemble, servent d'indicateurs de grossesse. Selon les achats de chaque cliente, il fut possible de calculer la possibilité qu'elle soit enceinte et de lui assigner une cote ; une sorte de pointage permettant de hiérarchiser les prédictions de la compagnie[2]. Ainsi, lorsqu'une cliente affichait une cote élevée, il était possible d'inférer avec un certain degré de précision qu'elle était enceinte et d'entamer le processus de personnalisation de l'offre publicitaire.

Cette brève anecdote illustre comment des renseignements personnels peuvent être analysés de manière à faire émerger un savoir sur certaines personnes ; un savoir que la personne pourrait s'attendre à garder secret, et qui peut être mobilisé pour agir sur son comportement. Bien qu'il soit difficile de déterminer si des techniques d'intelligence artificielle furent utilisées par Target, je tenterai de montrer, à la sous-section suivante, que ces techniques permettent, elles aussi, la mise en œuvre de cette logique particulière.

### 1.2 Que disent les données lorsque l'intelligence artificielle les fait parler ?

Au cours des dernières années, certaines techniques de traitement de l'information issues de l'intelligence artificielle furent utilisées par des équipes de chercheurs en psychologie afin de prédire

2. L'article de Duhigg utilise le terme de « pregnancy prediction score ».

certains attributs des personnes, comme leurs habitudes de vie, leurs préférences ou leurs traits de personnalité. L'objectif de ces équipes est de comprendre comment générer, à partir de données déjà existantes, de nouvelles informations au sujet des personnes. Plus précisément, il s'agit, comme dans l'anecdote de Target relatée plus haut, de prédire certains attributs et comportements lorsqu'il est possible d'observer et de confirmer l'existence de certains indicateurs de tendances plus générales. Pour ce faire, les chercheurs doivent collecter de vastes quantités de données, analyser ces données afin d'établir des corrélations empiriques leur permettant de faire des prédictions, et de vérifier la validité de ces prédictions[3].

Les données soumises aux différents algorithmes peuvent provenir de plusieurs sources, mais sont généralement extraites des traces numériques (*digital footprint*) que laissent derrière elles les personnes lorsqu'elles naviguent sur Internet ou utilisent leurs appareils intelligents. Ainsi, une première distinction, entre deux catégories de renseignements, s'impose : les données que l'on peut qualifier de « primaires », c'est-à-dire les renseignements, personnels ou non, qui sont générés par les personnes lorsqu'elles utilisent leurs appareils intelligents ou qu'elles naviguent sur Internet, et les données « émergentes », c'est-à-dire le savoir créé par le traitement des données primaires. L'objectif de cette sous-section est de décrire la nature des données émergentes qui peuvent être générées par le biais de techniques d'intelligence artificielle.

Dans un article percutant, Michal Kosinski, David Stillwell et Thore Greapel ont réussi à démontrer que des données primaires en apparence relativement banales, comme des « j'aime » sur Facebook[4], peuvent être utilisées pour générer un large éventail d'attributs personnels que les usagers n'ont pas nécessairement partagés ou divulgués, et qu'ils peuvent considérer comme privés ou secrets[5]. En analysant les « j'aime » de 58 000 volontaires au moyen de techniques d'apprentissage automatique, Kosinski et ses collègues ont réussi à prédire avec un haut degré de précision certains attributs personnels comme le genre, l'âge, la race, l'appartenance religieuse, les sensibili-

3. Wiebke BLEIDORN et Christopher James HOPWOOD, « Using Machine Learning to Advance Personality Assessment and Theory », (2018) 00:0 *Personality and Social Psychology Review* 1.
4. Il s'agit des fameux *likes* sur Facebook qui sont utilisés par les usagers afin de marquer leur appréciation d'une page, d'une image, d'un commentaire ou d'une vidéo.
5. Michal KOSINSKI, David STILLWELL et Thore GRAEPEL, « Private traits and attributes are predictable from digital records of human behavior », (2013) 110:15 *Proceedings of the National Academy of Sciences* 5802.

tés politiques, mais aussi certains faits relatifs aux habitudes et aux modes de vie des personnes, comme la consommation d'alcool ou de drogue et l'orientation sexuelle[6]. Les chercheurs furent finalement en mesure de déterminer certains traits de personnalité des personnes, comme la stabilité émotionnelle, l'intelligence, l'ouverture d'esprit ou l'amabilité[7]. En somme, l'étude de Kosinski et de ses collègues aura permis la création de profils psycho-démographiques détaillés à partir de données primaires relativement banales et qui sont faciles à collecter[8].

Les travaux de Kosinski et de ses collègues sur l'apprentissage automatique furent repris et revisités à maintes reprises. Par exemple, Park *et al.* ont évalué les données de 66 000 utilisateurs de Facebook à l'aide de techniques d'analyses linguistiques automatisées pour conclure que le vocabulaire employé par une personne peut contribuer à identifier et à mesurer certains traits de personnalité[9]. Youyou *et al.* ont montré que l'apprentissage automatique permet d'entraîner un modèle informatique à prédire les traits de caractère d'une personne de manière plus efficace qu'une personne humaine[10]. De même, Yilun Wang et Michal Kosinski ont analysé plus de 35 000 images faciales à l'aide de réseaux d'apprentissage profond pour découvrir que ces réseaux peuvent déterminer l'orientation sexuelle d'une personne avec un haut degré de certitude[11]. Youyou *et al.* ont également réussi à inférer certains attributs personnels et traits de personnalité d'une personne à partir de l'analyse de ses amis et de ses partenaires[12]. Finalement, Metz *et al.* ont conduit trois études menées auprès de 3,5 millions de personnes dans le but de démontrer que les publicités

6. *Ibid.*, p. 5803.
7. *Ibid.*, p. 5804.
8. *Ibid.*, p. 5805.
9. Gregory PARK, H. Andrew SCHWARTZ, Johannes C. EICHSTAEDT, Margaret L. KERN, Michal KOSINSKI, David J. STILLWELL, Lyle H. UNGAR et Martin E. P. SELIGMAN, « Automatic Personality Assessment Through Social Media Language », (2015) 108:6 J*ournal of Personality and Social Psychology* 934, p. 942-943.
10. Wu YOUYOU, Michal KOSINSKI, et David STILLWELL, « Computer-based personality judgments are more accurate than those made by humans », (2015) 112:4 *Proceedings of the National Academy of Sciences* 1036, p. 1039.
11. Yilun WANG et Michal KOSINSKI, « Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation From Facial Images », (2018) 114:2 *Journal of Personality and Social Psychology* 246, p. 247.
12. Wu YOUYOU, David STILLWELL, Andrew H. SCHWARTZ et Michal KOSINSKI, « Birds of a Feather Do Flock Together: Behavior-Based Personality-Assessment Method Reveals Personality Similarity Among Couples and Friends », (2017) 28:3 *Psychological Science* 276, p. 279-281.

ciblées conçues à partir de profils psycho-démographiques permettent de modifier de manière importante leurs comportements en ligne[13].

La revue de ces travaux révèle deux choses. Dans un premier temps, on remarque que les techniques d'apprentissage automatique et d'apprentissage profond permettent de dégager un savoir précis au sujet des personnes. Ce savoir se décline sous l'angle de la création de profils psycho-démographiques comprenant des prédictions relatives aux préférences, habitudes de vie et traits de personnalité des personnes. Or ces informations n'ont pas été explicitement partagées par les usagers, de sorte que les révélations qu'elles entraînent échappent au contrôle individuel que les personnes doivent être en mesure d'exercer sur leurs renseignements personnels. J'y reviendrai à la prochaine section[14].

Dans un second temps, le savoir psycho-démographique généré par l'intelligence artificielle est un savoir utile, c'est-à-dire qu'il s'agit d'un savoir mobilisable par différents acteurs désireux de comprendre les actions passées des personnes et d'orienter leurs comportements futurs. Bien que ce savoir puisse être utilisé pour des fins relativement banales, comme l'amélioration de produits ou la personnalisation de services, il peut aussi servir des intentions plus malveillantes. À cet effet, plusieurs auteurs expriment leurs craintes relativement aux risques de biais[15], de profilage[16], de discrimination[17] et de manipulation des opinions ou des comportements[18] qu'engendrent cette connaissance émergente, et dénoncent le contrôle qui peut alors être exercé

13. Sandra C. METZ, Michal KOSINSKI, G. NAVE et David STILLWELL, « Psychological targeting as an effective approach to digital mass persuasion », (2017) 114:18 *Proceedings of the National Academy of Sciences* 12714, p. 12 717.
14. Voir la section 2.2. du présent article.
15. Frank PASQUALE, *The Black Box Society. The Secret Algorithms that Control Money and Information*, Cambridge, Harvard University Press, p. 38 et s.
16. Antoinette ROUVEROY et Thomas BERNS, « Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation », (2012) 177:1 *Réseau* 165, p. 171.
17. B. BRODO, N. HELBERGER, K. IRION, K. ZUIDERVEEN BORGESIUS et J. MOLLER, « Tackling the Algorithmic Control Crisis – the Technical, Legal, and Ethical Challenges of Research into Algorithmic Agents », (2017) 19:1 *Yale Journal of Law and Technology* 133, p. 142 ; Amitai ETZIONO et Oren ETZIONI, « Keeping AI Legal », (2016) 19 *Vanderbilt Journal of Entertainment & Technology* 133, p. 138 et s. ; voir aussi WANG et KOSINSKI, *supra*, note 11.
18. Danny AZUCAR, Davide MARENGO et Michele SETTANI, « Predicting the Big 5 personality traits from digital footprints on social media: A meta-analysis », (2018) 124 *Personality and Individual Differences* 150, p. 157 ; Roberto J. GONZÁLEZ, « Hacking the citizenry? Personality profiling, "big data" and the election of Donald Trump », (2017) 33:3 *Anthropology Today* 9. Voir aussi Metz *et al.*, *supra*, note 13.

sur la vie des personnes[19]. On aura compris que, pour encadrer cette utilisation des données et prévenir les atteintes injustifiées à la vie privée des personnes, le droit à la protection des données personnelles sera appelé à jouer un rôle déterminant. Toutefois, le traitement des données personnelles à l'aide de techniques d'intelligence artificielle adopte une logique qui ne s'apparie que difficilement avec l'approche adoptée par la législation canadienne. Ce sera l'objet de la prochaine section que de discuter des limites du droit canadien en matière de protection des renseignements personnels à l'ère de l'intelligence artificielle.

## 2. LES LIMITES DE LA PROTECTION JURIDIQUE DES PERSONNES ET DES RENSEIGNEMENTS PERSONNELS

Dans cette section, j'identifie certains des défis que la création de données émergentes pose au droit à la vie privée informationnelle. L'ensemble des lois de protection des renseignements personnels canadiennes sont construites dans une optique relativement similaire. L'objectif de ces lois est de permettre aux personnes d'exercer un contrôle sur les modalités de circulation et de diffusion de leurs renseignements personnels. Cette notion de contrôle est opérationnalisée au moyen du principe de consentement ; sauf exception, la personne doit être en mesure de consentir au traitement de ses renseignements personnels. Pour que ce consentement soit valide, il faut que la personne comprenne pourquoi ses renseignements sont traités. Ainsi, les lois canadiennes prévoient que les entités qui souhaitent traiter des renseignements personnels doivent préalablement établir les fins visées par le traitement, et informer les personnes de ces fins avant que le traitement ne commence. Les techniques d'intelligence artificielle remettent en question plusieurs des éléments de cette approche. Je retiens ainsi trois principales limites du droit à la vie privée : une limite ontologique qui porte sur la protection des groupes algorithmiques (2.1), une limite opérationnelle qui porte sur la créa-

19. On retrouve dans la littérature relative à l'intelligence artificielle, aux nouvelles technologies et à la vie privée un courant qui s'intéresse à la cristallisation de ce que Gilles Deleuze nommait les sociétés de contrôle, c'est-à-dire de sociétés où un contrôle ex ante et continu est exercé sur les individus. Bien qu'une revue exhaustive des travaux qui portent sur cette question serait ici trop longue, nous référons le lecteur à certains textes porteurs : Gilles DELEUZE, « Postscript on the Societies of Control », (1992) 59 *October* 3 ; Primavera DE FILIPPI et Aaron WRIGHT, *Blockchain and the Law. The Rule of Code*, Cambridge, Harvard University Press, 2018, p. 52 et s. ; voir aussi ROUVEROY et BERNS, *supra*, note 16, p. 180 et s.

tion des données émergentes (2.2) et une limite structurelle qui porte sur le cycle de traitement de l'information (2.3).

### 2.1 La limite ontologique : la protection des groupes algorithmiques

La première limite que je retiens est une limite ontologique ; elle s'intéresse aux entités qui, pour le droit canadien, existent, peuvent exister ou n'existent pas. Comme discuté plus haut, les lois canadiennes visent la protection des personnes et ont comme objectif d'encadrer le traitement des renseignements personnels. Pour ces lois, seules les personnes identifiables et les renseignements qui concernent ces personnes sont protégés. Or, à l'ère de l'intelligence artificielle, ce niveau élémentaire de protection, centré sur la personne et sur ses renseignements, s'avère largement insuffisant. En effet, de nouvelles classes d'entités, jusqu'à présent largement ignorées par le droit, doivent être prises en charge ; les groupes algorithmiques et les renseignements dépersonnalisés.

L'idée de s'intéresser à la protection de la vie privée des groupes n'est pas nouvelle[20]. Toutefois, la théorie de la vie privée s'est traditionnellement penchée sur des groupes identitaires, c'est-à-dire des groupes dont les lignes de contour s'articulent en fonction de variables politiques, religieuses ou culturelles. Les groupes dont il est aujourd'hui question sont des groupes d'un autre ordre. Il ne s'agit pas de groupes identitaires, mais bien de groupes qualifiés dans la littérature de groupes algorithmiques ; des groupes virtuels, artificiels, qui sont désignés, construits de toutes pièces par des procédés algorithmiques[21]. Contrairement aux groupes identitaires, les membres d'un groupe algorithmique ne savent pas qu'ils appartiennent à ce groupe ni même que ce groupe existe[22]. Pensons, notamment, à l'exemple du groupe des femmes enceintes créé par Target[23].

Les groupes algorithmiques sont généralement créés à partir de l'analyse de données déjà collectées, des données disponibles qui

20. Sur ce point, voir Edward J. BLOUSTEIN, *Individual and Group Privacy*, New York, Transaction Publishers, 1978.
21. Sur ce point, voir les excellents ouvrages de Linnet TAYLOR, Luciano FLORIDI et Bart VAN DER SLOOT (dir.), *Group Privacy: New Challenges of Data Technologies*, Dordrecht, Springer, 2017 et de Bart VAN DER SLOOT, *Privacy as Virtue. Moving Beyond the Individual in the Age of Big Data*, Amsterdam, Intersentia, 2017 ; voir aussi Luciano FLORIDI, « Open Data, Data Protection, and Group Privacy », (2014) 27:1 *Philosophy and Technology* 1.
22. Voir aussi ROUVEROY et BERNS, *supra*, note 16, p. 171.
23. Voir la section 2.1 du présent article.

seront couplées et croisées de manière à faire émerger des tendances générales, des mouvements plus systémiques, plus macroscopiques. Le but est d'identifier des points de convergence entre les données – par exemple, tous les produits achetés par les femmes enceintes. Ce nouveau traitement de l'information crée des profils types, des identités génériques qui peuvent servir de grilles de lectures des personnes. Le groupe, ici, c'est donc l'ensemble des personnes qui affichent les caractéristiques qui correspondent à cette identité générique, qui rentrent dans ce moule ou qui, si on me permet l'expression, « *fit* le profil ».

Deux constats méritent d'être brièvement discutés. Le premier constat est que la création de ces groupes algorithmiques ne nécessite pas le traitement de renseignements personnels au sens juridique du terme. Il s'agit certes de données qui portent sur les personnes, mais le fait que ces personnes soient identifiables[24] ne revêt pas une importance fondamentale[25]. En fait, l'identité des personnes joue un rôle que l'on peut qualifier de secondaire. Ce qui intéresse certaines organisations, c'est l'appartenance des personnes à différents groupes, et ce que cette appartenance peut dire sur elles. De même, les groupes algorithmiques peuvent très bien être créés à partir de renseignements dépersonnalisés ou de renseignements qui se rapportent à des pseudo-identités[26].

Cela m'amène au second constat. La création de groupes algorithmiques amplifie le principe de « l'effet réseau » ou du « *network effect* » en anglais. Le principe de l'effet réseau est simple : il se manifeste lorsque les actions d'une personne relativement à sa vie privée produisent des effets sur la vie privée d'une ou plusieurs autres personnes. L'exemple classique est celui de la publication sur un réseau social d'une photographie d'un groupe d'amis qui assistent au même évènement. La publication de l'image par un des membres du groupe révèle certaines informations qui concernent tous les autres

---

24. En droit à la vie privée canadien, la capacité d'identifier une personne est fondamentale. En effet, seuls les renseignements qui portent sur une personne identifiable sont considérés comme des renseignements personnels et sont donc protégés. Voir, par exemple, la définition de « renseignements personnels » dans la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5, [LPRPDE] article 2 où la notion de renseignement personnel est définie comme « [t]out renseignement concernant un individu identifiable ».
25. Voir sur ce point, Linnet TAYLOR, Luciano FLORIDI et Bart VAN DER SLOOT, « Introduction: A New Perspective on Privacy », dans TAYLOR, FLORIDI et VAN DER SLOOT, *supra*, note 21.
26. Voir Linnet TAYLOR, « Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World », dans TAYLOR, FLORIDI et VAN DER SLOOT, *supra*, note 21 ; voir aussi Metz *et al.*, *supra*, note 13.

membres : il est possible de dire où ils étaient à ce moment précis, avec qui ils étaient et peut-être même pourquoi.

Dans le contexte des groupes algorithmiques, ce principe de l'effet réseau opère d'une manière similaire. Un groupe algorithmique est initialement créé par le traitement et l'analyse d'un nombre fini de renseignements qui concernent un nombre fini de personnes. La connaissance qui est extraite du traitement et de l'analyse de ces renseignements n'est toutefois pas simplement applicable aux personnes qui composaient l'échantillon initial, mais est généralisable et transposable à l'ensemble des personnes qui partagent les mêmes caractéristiques que celles de la population de base. Ainsi, ce savoir émergent peut être applicable à des personnes dont les renseignements ne furent pas initialement partagés ou analysés. Par conséquent, même dans l'éventualité où le profil type est créé à partir de renseignements qui furent partagés volontairement et en toute connaissance de cause par certaines personnes, la connaissance « toute faite » qu'il véhicule pourra être superposée à de nouvelles personnes qui n'ont pas consenti au traitement informationnel initial.

Pour bien comprendre la portée de ces deux constats, l'anecdote de la jeune femme enceinte m'apparaît pertinente. Rappelons-nous que c'est en analysant les renseignements portant sur des femmes que la compagnie savait enceintes que Target fut en mesure d'identifier les 25 produits dont l'achat serait indicatif d'une grossesse. Dans le cas de Target, les renseignements traités étaient des renseignements personnels au sens juridique, c'est-à-dire qu'ils portaient sur des femmes identifiables, associées à des comptes clients comprenant, entre autres, leur nom, leur adresse et leurs numéros de carte de crédit. Mais il est aussi possible, comme mentionné plus haut[27], de créer et de partager ces groupes à partir de renseignements qui sont dépersonnalisés[28].

Au Canada, les renseignements dépersonnalisés sont exclus de la sphère de protection de l'ensemble des lois portant sur la protection des renseignements personnels[29]. Ces renseignements peuvent géné-

27. *Ibid*.
28. Notons aussi que plusieurs géants du Web partagent, pour des fins de publicité ciblée, des renseignements qui sont dépersonnalisés.
29. Voir, par exemple, LPRPDE, *supra*, note 24, annexe 1, principe 4.5.3. Comme un renseignement personnel est un renseignement qui concerne un individu identifiable, un renseignement dépersonnalisé – c'est-à-dire un renseignement transformé de manière à ce qu'il ne révèle plus directement l'identité de la personne – n'est pas, par définition, un renseignement personnel. Voir aussi, les lois de l'Alberta, *Health Information Act*, R.S.A. 2000, c. H-5, art. 1, 19, 26, 32, 57(1) et 57(2); de la Saskatchewan, *The Health Information Protection Act*,

ralement être collectés, utilisés et communiqués sans le consentement de la personne. De plus, les critères à satisfaire pour qualifier un renseignement de « dépersonnalisé » sont à la fois vagues et difficilement applicables[30], et peuvent varier d'une juridiction à l'autre[31]. Notons aussi que, même si le traitement de renseignements dépersonnalisés peut dans une certaine mesure assurer une meilleure protection de la vie privée des personnes, la possibilité de ré-identification des personnes, et par conséquent d'immixtion dans la sphère intime des personnes, est toujours présente. De surcroît, on peut imaginer que cette capacité à ré-identifier les personnes au sujet desquelles un savoir important est déjà amassé viendra titiller certaines entités malveillantes ou plus malicieuses. Par conséquent, le fait que le droit canadien ne protège que les renseignements personnels, c'est-à-dire les renseignements qui portent sur une personne identifiable, et qu'il semble ignorer les entités que sont les groupes algorithmiques, représente une limite ontologique importante.

### 2.2 La limite opérationnelle : le contrôle sur les renseignements et le principe du consentement individuel

La seconde limite que je retiens est une limite opérationnelle ; elle s'intéresse à l'incapacité des personnes à exercer un contrôle efficace sur les modalités de circulation et de diffusion de leurs renseignements personnels. Le droit à la vie privée canadien est en grande partie construit autour de la notion de contrôle individuel. Protéger la vie privée, c'est protéger la capacité des personnes à exercer un contrôle sur leurs renseignements personnels ; à décider quand, à

---

S.S. 1999, c. H-0.021, art. 29(2)a), 3(12)a), 23(4) 26(2)b) ; du Manitoba, *Loi sur les renseignements médicaux personnels*, C.P.L.M., c. P-33.5, art. 22(2)g3), 21c)(i) et art. 3 ; de l'Ontario, *Loi de 2004 sur la protection des renseignements personnels sur la santé*, L.O. 2004, c. 3 art. 47(1) 55.9)3) et (4) ; du Nouveau-Brunswick, *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé*, L.R.N.-B. 2009, c. P-7.05, art. 3(2)a), 30, 33, 34(1)h, 34(1)o)iii), 36 et 51 ; de la Nouvelle-Écosse, *Personal Health Information Act*, S.N.S. 2010, c. 41, art. 3g) 5(1) et 49(2) ; de Terre-Neuve et du Labrador, *Personal Health Information Act*, S.N.L. 2008, c. P-7.01, art. 34p) ; et de l'Île-du-Prince-Édouard, *Health Information Act*, R.S.P.E.I. 2014, c. H-1.41, art. 20, 22(5)(h), 23(4) et 40.

30. Par exemple, dans *Gordon* c. *Canada (Santé)*, 2008 CF 258, par. 34 et s., un renseignement ne sera pas considéré comme personnel s'il n'y a pas de « fortes possibilités » qu'il permette d'identifier la personne.

31. Cette affirmation s'avère surtout vraie dans le contexte de la santé où les provinces de l'Ontario, du Nouveau-Brunswick, de la Nouvelle-Écosse et de la Saskatchewan ont adopté le critère du « raisonnablement possible » de prévoir que les renseignements permettront de révéler l'identité des personnes sources. En Alberta, à l'Île-du-Prince-Édouard et au Manitoba, c'est le critère de la « facilité » qui fut retenu.

qui, pourquoi et comment les renseignements qui les concernent sont transmis. Cette notion de contrôle est opérationnalisée au moyen du principe du consentement. En règle générale, les renseignements d'une personne ne peuvent être collectés, utilisés ou communiqués qu'avec le consentement de la personne.

L'idée que les personnes éprouvent d'importantes difficultés à exercer un contrôle efficace sur leurs renseignements personnels dans les environnements numériques n'est ni nouvelle[32] ni complètement étrangère au droit canadien[33]. Une des principales difficultés, et qui me semble exacerbée par la puissance prédictive des techniques de traitement de l'information discutées plus haut[34], est le fait que les personnes génèrent, souvent sans le savoir, une quantité extraordinaire de données, et ce, simplement en utilisant leurs appareils intelligents ou en naviguant sur Internet. Les mots clés inscrits sur les moteurs de recherche, les liens cliqués, la durée et la fréquence des visites sur les pages, les « j'aime » sur Facebook, les « retweet » sur Twitter sont des exemples de données primaires qui sont générées par les personnes et collectées de manière presque systématique par les acteurs du Web.

Face à ce constat, deux séries de questions s'imposent. La première porte sur la validité du consentement individuel à la collecte, l'utilisation et la communication des données primaires qui composent les traces numériques des personnes. Les personnes peuvent-elles comprendre les modalités du traitement algorithmique de l'information ? Comment réfléchir le consentement individuel si peu de personnes lisent les conditions d'utilisation et les politiques de confidentialité des services en ligne[35] ? Peut-on réellement parler d'un consentement libre et éclairé ? Que faire des cas où le consentement n'est même pas sollicité ? Ces questions furent largement traitées

32. Voir, entre autres, Solon BAROCAS et Helen NISSENBAUM, « Big Data's End Run around Anonymity and Consent », dans Julia LANE, Victoria STODDEN, Stefan BENDER et Helen NISSENBAUM (dir.), *Privacy, Big Data, and the Public Good Frameworks for Engagement*, Cambridge, Cambridge University Press, 2016 ; voir aussi Pierre TRUDEL, « La protection de la vie privée dans les réseaux : des paradigmes alarmistes aux garanties effectives », (2006) 61:7-8 *Annales des télécommunications* 950.
33. Voir, par exemple, *R.* c. *Vu*, [2013] 3 R.C.S. 657, par. 42.
34. Voir la section 1.2 du présent article.
35. Un sondage de 2016 du Commissariat à la protection de la vie privée du Canada montre que seulement 40 % des Canadiens et Canadiennes lisent les politiques de confidentialité se rapportant aux applications qu'ils utilisent. Voir le Sondage auprès des Canadiens sur la protection de la vie privée de 2016, 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/2016/por_2016_12/>.

ailleurs[36] et, bien qu'elles demeurent ici pertinentes, je ne crois pas nécessaire de les aborder à nouveau. La seconde série de questions, qui m'intéresse davantage, porte sur la perte de contrôle qu'engendre non pas la collecte des données primaires, mais l'extraction de connaissances sur les personnes à partir de ces données. Ces données émergentes n'ont pas été initialement partagées par les personnes, et celles-ci ne peuvent raisonnablement s'attendre à ce qu'elles soient révélées. Cet enjeu est d'autant plus problématique dans les cas où les données primaires ont été glanées sans le consentement de la personne. Comme l'expliquent Metz *et al.* dans un passage qui rappelle certains des enjeux évoqués à la section 2.1, les personnes peuvent révéler beaucoup plus que ce qu'elles anticipaient initialement :

> Although we used indirect group-level targeting in a way that was anonymous at the individual level and thus preserved — rather than invaded — participants' privacy, the same approach could also be used to reveal individuals' intimate traits without their awareness. For example, a company could advertise a link to a product or a questionnaire on Facebook, targeting people who follow a Facebook Like that is highly predictive of introversion. Simply following such a link reveals the trait to the advertiser, without the individuals being aware that they have exposed this information. […] Our empirical experiments were performed without collecting any individual-level information whatsoever on our subjects yet revealed personal information that many would consider deeply private.[37]

Selon plusieurs chercheurs, et je partage cet avis, ces immixtions non consenties dans la sphère privée de la personne peuvent et doivent être considérées comme de dangereuses atteintes à la vie privée[38]. Toutefois, les problèmes du consentement et de la perte de contrôle des personnes sur leurs renseignements personnels ne se manifestent pas seulement dans les cas où les données primaires sont collectées et analysées sans le consentement des personnes. Les entités qui souhaitent obtenir un consentement éclairé des personnes éprouveront souvent de grandes difficultés à fournir des explications claires et digestes sur les fins qu'elles visent par le traitement de

---

36. En 2016, le Commissariat à la protection de la vie privée du Canada a entamé une vaste campagne de consultation sur le principe du consentement. Les résultats de cette campagne sont disponibles en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultation-sur-le-consentement-en-vertu-de-la-lprpde/>.
37. METZ *et al.*, *supra*, note 13, p. 12 717.
38. KOSINSKI, STILLWELL et GRAEPEL, *supra*, note 5, p. 5 802 et WANG et KOSINSKI, *supra*, note 11, p. 255.

renseignements personnels. Cela tient, en partie, au fait que les algorithmes d'intelligence artificielle fonctionnent de manière opaque et que leurs modes de fonctionnement interne sont difficilement interprétables[39]. D'une manière peut-être plus importante, ces difficultés tiennent aussi au fait que, dans le domaine de l'intelligence artificielle, les fins visées par le traitement des données primaires ne sont pas toujours claires ou facilement identifiables. Pour bien comprendre cette dernière affirmation, il est nécessaire de voir en quoi le mode opératoire de création de la connaissance dans le domaine de l'intelligence artificielle diffère des techniques scientifiques normales. Ce sera l'objet de la prochaine sous-section que de discuter de cette idée.

### 2.3 La limite structurelle : le cycle de traitement de l'information

La dernière limite que je retiens est une limite que je qualifie de structurelle. Les lois de protection des renseignements personnels canadiennes sont toutes construites autour d'un cycle de traitement de l'information particulier, qui vient structurer la séquence d'actions que doit suivre une entité souhaitant traiter des renseignements personnels. En règle générale, l'entité doit d'abord identifier la fin qu'elle poursuit par le traitement de l'information et, ensuite, informer la personne de cette fin. C'est cette explication qui permet d'asseoir le caractère éclairé du consentement individuel. Lorsqu'elle obtient ce consentement, l'entité pourra collecter les renseignements nécessaires à l'atteinte de cette fin, utiliser ces renseignements dans l'atteinte de cette fin et communiquer ces renseignements si cette communication s'inscrit dans la visée de cette fin.

Ce cycle particulier de traitement de l'information me semble calqué sur le mode opératoire de la science moderne ; on pose une question et formule une hypothèse plausible et falsifiable, on identifie et collecte les données qui seront nécessaires pour mettre à l'épreuve notre hypothèse, on analyse ces données et répond à la question. Or, comme mentionnée à la sous-section précédente, l'extraction de connaissances dans le domaine de l'intelligence artificielle ne suit pas cette logique particulière. Dans le contexte de l'intelligence artificielle, l'analyse des données débute souvent avant même qu'une question ne soit posée ou qu'une hypothèse ne soit formulée[40]. En fait, ce sera le traitement de l'information par le biais des techniques d'intelli-

39. Voir, entre autres, PASQUALE, *supra*, note 15, p. 7 et s. et W. NICHOLSON PRICE II, « Black-Box Medicine », (2015) 28:2 *Harvard Journal of Law & Technology* 420, p. 432 et s.
40. BLEIDORN et HOPWOOD, *supra*, note 3, p. 2.

gence artificielle qui permettront de détecter, à travers un champ de possibilités, les hypothèses plausibles qui guideront l'élaboration de prédictions[41].

Les *big data* de l'intelligence artificielle auront catalysé la dissémination de modes de création de la connaissance qui semblent moins guidés par des finalités et des idées que par les possibilités offertes par les données elles-mêmes[42]. En raison de leur grande disponibilité et de leurs faibles coûts d'acquisition, les données soumises à l'analyse seront donc souvent collectées avant même qu'une finalité de traitement soit identifiée[43], de sorte que le contexte d'application des résultats générés ne sera identifié qu'une fois l'analyse terminée[44]. Qui plus est, l'apprentissage continu auquel se livrent les techniques d'intelligence artificielle exige de nouvelles et fréquentes vagues de collecte de données permettant de vérifier et d'augmenter le degré de certitude des prédictions générées. Les étapes de collecte, d'utilisation et de divulgation des renseignements personnels, prévues de manières successives et distinctes par la loi, sont effectuées de manière presque simultanée et semblent difficilement dissociables dans le domaine de l'intelligence artificielle.

Comme discuté plus tôt dans cet article, l'intelligence artificielle permet la création de groupes algorithmiques, de profils et d'identités génériques à partir de données dépersonnalisées qui, par définition, sont exclues de la sphère de protection offerte par la loi. Ce savoir préexistant peut être récupéré et utilisé pour mieux connaître des personnes au sujet desquels on possède déjà certains renseignements et exercer sur elles une certaine influence. Ces deux jeux de données, produits tous deux par différentes collectes de données personnelles et différents processus de traitement de l'information, se voient donc raboutés, scellant un processus opérant par boucles et contribuant à la perte de contrôle des personnes sur leur vie privée.

---

41. Comme le soulignent Antoinette Rouveroy et Thomas Berns,
Le propre de ce qu'on appelle le *machine learning* est somme toute de rendre directement possible la production d'hypothèse à partir des données elles-mêmes. De la sorte, nous nous trouvons à nouveau face à l'idée d'un savoir dont l'objectivité pourrait paraître absolue, puisqu'il serait éloigné de toute intervention subjective (de toute formulation d'hypothèse, de tout tri entre ce qui est pertinent et ce qui ne serait que du « bruit », etc.). Les normes semblent émerger directement du réel lui-même » (ROUVEROY et BERNS, *supra*, note 16, p. 70).
42. Voir, sur ce point, Douglas B. KELL et Stephen G. OLIVER, « Here is the Evidence, now what is the hypothesis? The complementary roles of inductive and hypothesis-driven science in the post-genomic era », (2003) 26:1 *BioEssays* 99.
43. BLEIDORN et HOPWOOD, *supra*, note 3, p. 2.
44. Chris ANDERSON, « The End of Theory: The Data Deluge Makes the Scientific Method Obsolete », *Wired*, 23 juin 2008, en ligne : <https://www.wired.com/2008/06/pb-theory/>.

Ici aussi, l'anecdote de Target et de la femme enceinte me semble particulièrement illustrative.

On aura compris que, dans un tel contexte, le respect de la marche à suivre mise en place par les lois canadiennes est difficile. Comment, en effet, bien informer les personnes des fins visées par le traitement de leurs renseignements personnels alors qu'on ne sait pas encore ce que l'on cherche exactement ? Comment obtenir un consentement éclairé des personnes ? De même, comment assurer le contrôle individuel sur les renseignements alors qu'il n'est pas tout à fait possible de savoir ce qui sera découvert avant que l'analyse des renseignements personnels ne soit complétée ? Face au développement des techniques d'intelligence artificielle, le droit à la vie privée me semble donc limité par sa structure opératoire même, une structure qui ne cadre plus avec les réalités contemporaines du traitement algorithmique de l'information.

## CONCLUSION

Dans cet article, j'ai tenté d'expliquer comment les techniques d'intelligence artificielle posent de sérieux défis au droit à la vie privée canadien. Pour conclure, il m'apparaît nécessaire d'évoquer certains développements juridiques récents relevant, en partie, ces défis. Les droits émergent dans des contextes particuliers, et, face à de nouvelles problématiques, de nouveaux droits sont parfois créés. Le droit à la vie privée n'échappe pas à cette logique[45]. Au cours des dernières années, de nouveaux droits visant la protection de la vie privée informationnelle des personnes firent leur apparition : droit à l'explication, droit à la portabilité des données et le fameux droit à l'oubli. Ces droits, qui ne se sont pas encore frayé un chemin au Canada, pourraient aider les personnes à mieux protéger leur vie privée dans les environnements numériques. Toutefois, je crois que, pour répondre aux défis soulevés dans cet article, le droit à la vie privée ne peut agir seul, et que d'autres pans du droit peuvent et doivent être mobilisés.

Bien que je ne pense pas que la notion du contrôle individuel est complètement obsolète, et que je continue de croire qu'il est possible de construire un modèle de consentement plus dynamique, plus

45. Voir, sur ce point, l'excellent article de Graham MAYEDA, « My Neighbour's Kid Just Bought a Drone... New Paradigms for Privacy Law in Canada », (2016) 35:1 *National Journal of Constitutional Law* 59.

fluide et mieux adapté aux réalités technologiques contemporaines[46], je reconnais que le cadre actuel comprend d'importantes limites. Face à la grande disponibilité de renseignements personnels déjà collectés, il peut être judicieux de porter une attention particulière aux utilisations de ces données. En d'autres mots, comme le soutient Frank Pasquale, il est peut-être temps de se résoudre à déplacer le curseur de l'intervention législative de la collecte des renseignements à l'utilisation de ces renseignements[47]. Cette solution interpelle des outils juridiques qui existent déjà, et qui se trouvent à l'extérieur du droit à la vie privée. Par exemple, le Canada a récemment adopté une loi[48] qui interdit l'utilisation de renseignements génétiques qui peut mener à certaines formes de profilage et de discrimination. Il s'agit donc de déterminer comment on peut baliser l'utilisation du savoir généré par l'intelligence artificielle et de s'intéresser au développement responsable, positif et éthique des techniques de traitement de l'information issues de ce domaine. En somme, il s'agit de se rappeler que le droit ne sert pas à protéger les renseignements, mais bien les personnes et toutes les dimensions de leur vie.

46. Voir, par exemple, Saskia C. SANDERSON *et al.*, « Public Attitudes toward Consent and Data Sharing in Biobank Research: A Large Multi-site Experimental Survey in the US », (2017) 100 *The American Journal of Human Genetics* 414.
47. PASQUALE, *supra*, note 15, p. 141.
48. *Loi sur la non-discrimination génétique*, L.C. 2017, c. 3.