LA VIE PRIVÉE DES GROUPES : NOUVEAU CADRE THÉORIQUE POUR UNE PROTECTION CONTRE LE PROFILAGE ALGORITHMIQUE

Simon DU PERRON[1]

1 L'auteur est candidat à la Maîtrise en droit des technologies de l'information à la Faculté de droit de l'Université de Montréal et assistant de recherche au Laboratoire de cyberjustice.

Résumé

On observe un fossé de plus en plus grand entre d'une part, les modèles d'affaires qui misent sur l'exploitation des mégadonnées afin de catégoriser les individus en fonction de leur correspondance à différents profils algorithmiques, et de l'autre, un paradigme juridique axé sur l'individu. La vie privée des groupes est un nouveau cadre théorique multidisciplinaire qui s'inscrit en réponse à ce décalage. Le « groupe algorithmique » constitue un nouveau phénomène épistémologique généré par les nombreuses opérations de classification et d'agrégation à l'œuvre au sein des mégadonnées. Ces regroupements s'effectuent principalement à partir de données anonymisées ou dépersonnalisées de sorte que les individus sont rarement conscients de leur appartenance à un groupe algorithmique. Considérant les préjudices que le traitement algorithmique des données peut causer aux membres du groupe, mais également pour le groupe *en tant que groupe*, il importe d'élargir la portée du droit à la vie privée et de reconnaître l'intérêt collectif d'être protégé contre le profilage algorithmique. Les travaux d'auteurs qui abordent le droit à la vie privée dans une perspective antidiscriminatoire, ainsi qu'une interprétation novatrice de l'article 8 de la *Convention européenne des droits de l'Homme,* constituent un bon point de départ pour articuler une théorie permettant de reconnaitre un droit collectif à la vie privée des groupes.

INTRODUCTION

> *Sometimes the only way to protect the individual is to protect the group to which the individual belongs. Preferably before any disaster happens.*
>
> - Luciano Floridi, "Open Data, Data Protection, and Group Privacy"[2]

[1] Tout autour de nous, les technologies numériques scrutent et enregistrent des facettes de nos vies : les endroits que nous visitons, les sites web que nous consultons, les téléséries que nous regardons, etc. L'exploitation de ces mégadonnées (*big data*) caractérise le modèle d'affaires des géants du numérique[3], décrit par Shoshana Zuboff comme un capitalisme de surveillance qui cherche à traduire toute expérience humaine en information pouvant servir de valeur marchande pour les entreprises qui la détiennent et savent l'exploiter[4]. Dans ce contexte marqué par des techniques d'analyse des données conçues pour opérer à la plus large échelle possible[5], force est d'admettre que les données *personnelles* n'occupent en réalité qu'une place anecdotique[6].

[2] Or, le droit à la vie privée demeure strictement axé sur l'individu et l'ensemble des outils élaborés pour protéger la vie privée lui sont destinés[7]. On observe un fossé de plus en plus grand entre d'une part, l'exploitation des mégadonnées afin de catégoriser les individus en fonction de leur correspondance à différents profils algorithmiques[8], et de l'autre, un paradigme juridique axé sur l'individualité. C'est en réponse à ce décalage que s'inscrit la vie privée des groupes (*group privacy*) : un nouveau cadre théorique multidisciplinaire développé dans l'ouvrage *Group Privacy New Challenges of Data Technologies*[9].

2 Luciano Floridi, « Open Data, Data Protection, and Group Privacy » (2014) 27-1 *Philosophy & Technology*

3 Groupe d'examen du cadre législatif en matière de radiodiffusion et de télécommunications, *L'avenir des communications au Canada : le temps d'agir*, Ottawa, 2020, p. 210.

4 Shoshana Zuboff, *The Age of Surveillance Capitalism,* 1re éd., New York, PublicAffairs, 2019.

5 "In many areas, however, a shift is taking place from collecting some data to gathering as much as possible, and, if feasible, getting everything : *N =all*." (Viktor Mayer-Schönberger et Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Boston, Houghton Mifflin Harcourt Publishing Company, 2013, p. 26.)

6 Antoinette Rouvroy, « Des données sans personne: le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des Big Data », (2014) *Étude annuelle 2014 - Le numérique et les droits fondamentaux*, p. 8.

7 Karim Benyekhlef et Pierre-Luc Déziel, Le droit à la vie privée en droit québécois et canadien, Montréal, Éditions Yvon Blais, 2018, p. 51.

8 Moritz Büchi et al., « The chilling effects of algorithmic profiling: Mapping the issues », (2020) 36 *Computer Law & Security Review* 1.

9 Linnet Taylor, Luciano Floridi et Bart van der Sloot (dir.), *Group Privacy: New Challenges of Data Technologies,* Dordrecht, Springer, 2017 (ci-après « *Group Privacy* »).

I – LA VIE PRIVÉE DES GROUPES : QUAND PROTÉGER L'INDIVIDU NE SUFFIT PLUS

I.1. QU'EST-CE QU'UN « GROUPE » ?

[3] Le mot « groupe » réfère généralement à un ensemble de personnes formant un tout et défini par une caractéristique commune[10]. Cependant, pour bien saisir la notion de vie privée des groupes, il importe de distinguer le groupe « actif » du groupe « passif »[11].

[4] Le groupe actif est composé d'individus qui sont conscients de leur appartenance au groupe et qui s'y identifient. Ces membres partagent certaines caractéristiques, ainsi qu'un certain historique d'interactions et/ou d'objectifs en commun. Le groupe actif requiert un certain niveau de conscience *collective*, ce qui ne signifie pas pour autant que tous ses membres se connaissent. Les étudiants d'une même Faculté, les membres d'un club de l'âge d'or, la communauté chinoise de l'île de Montréal, sont autant d'exemples de groupes actifs. Inversement, les membres d'un groupe passif ne sont pas nécessairement conscients de leur appartenance au groupe, car l'existence du groupe dépend de l'externe ; c'est le regard des autres qui lui donne naissance. Bien qu'ils puissent partager certaines caractéristiques en commun (ex. le fait de posséder une voiture rouge), les membres d'un groupe passif n'ont aucune intention d'exister en tant que collectivité. Les « personnes âgées » ou les « personnes vulnérables » par exemple, comptent des individus pouvant ne pas s'identifier au groupe, mais néanmoins en faire partie aux yeux du public.

[5] Parmi les groupes passifs, le groupe qui retiendra davantage notre attention en lien avec la théorie de la vie privée des groupes est le « groupe algorithmique » que Linnet Taylor décrit comme « un nouveau phénomène épistémologique généré par l'analyse des mégadonnées »[12]. Le groupe algorithmique est le fruit des nombreuses classifications opérées par les différents algorithmes à l'œuvre au sein des mégadonnées[13]. Le groupe désigne ici l'ensemble des individus qui

10 Larousse, « Définitions : groupe - Dictionnaire de français Larousse », en ligne : <https://www.larousse.fr/dictionnaires/francais/groupe/38423>.

11 Cette typologie nous est inspirée par les textes suivants : Lanah Kammourieh et al., « Group Privacy in the Age of Big Data », dans *Group Privacy*, préc. note 9, p. 38 à 40 et Michele Loi et Markus Christen, « Two Concepts of Group Privacy », (2019) *Philosophy & Technology* 18, p. 2.

12 Linnet Taylor, « Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World » dans *Group Privacy*, préc. note 8, p. 14.

13 À ce sujet, voir l'article de Nancy J. King et Jay Forder, « Data analytics and consumer profiling: Finding appropriate privacy principles for discovered data », (2016) 32-5 *Computer Law & Security Review* 696–714.

correspondent à certains profils déterminés par l'analyse des données (ex. les consommateurs ayant un intérêt pour le jardinage, les mères monoparentales vivant en secteur urbain, les parents en attente de leur premier enfant, etc.[14]). Notons que les regroupements algorithmiques s'effectuent principalement à partir de données anonymisées ou dépersonnalisées de sorte que les individus sont rarement conscients de leur appartenance à un groupe algorithmique ni de ses conséquences.

[6] Précisons que la classification entre groupe actif et groupe passif n'est pas immuable. Ainsi, l'algorithme de Netflix crée un groupe passif (et algorithmique) lorsqu'il regroupe certains utilisateurs sous la catégorie « Amateurs de films d'horreur ». Si Netflix mettait en place un forum destiné aux fans, le groupe deviendrait de plus en plus « actif » au fur et à mesure que les utilisateurs interagissent, s'organisent et partagent un sens du « nous ».

I.2 – EST-CE QUE LES « GROUPES » PEUVENT ÊTRE TITULAIRES DE DROITS?

[7] Reconnaitre des droits aux groupes implique de leur conférer la personnalité juridique. À ce sujet, Ugo Pagallo rappelle que le droit permet l'octroi de droits à des entités non humaines dont la configuration interne est appelée à changer[15]. On pense immédiatement aux personnes morales[16], mais l'histoire enseigne que des temples ont été considérés comme des sujets de droit dans la Rome antique[17]. Récemment, la personnalité juridique a été reconnue à l'égard d'un fleuve[18], de la forêt amazonienne[19] et l'on s'interroge à savoir si l'on devrait faire de même avec les agents autonomes[20].

14 Il s'agit de trois catégories utilisées par les courtiers en données américains pour définir des segments spécifiques de la population sur la base de l'analyse des mégadonnées (Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability*, 2014, en ligne : <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>).

15 Ugo Pagallo, « The Group, the Private, and the Individual: A New Level of Data Protection? » dans *Group privacy,* préc. note 9, p. 161.

16 *Code civil du Québec,* RLRQ, c. C-12, art. 298.

17 John Chipman Gray, *The Nature and Sources of the Law*, New Orleans, Quid Pro, 2012, p. 45.

18 En 2016, la Cour constitutionnelle de Colombie a reconnu la personnalité juridique au fleuve Atrato (Cour constitutionnelle colombienne, [2016] T-622) .

19 En 2018, la Cour suprême de Colombie a reconnu le statut de sujet de droit à la forêt amazonienne (El Tiempo Editorial, « Declaran la Amazonia sujeto de derechos para atacar la deforestación », *El Tiempo*, 5 avril 2018, en ligne : <https://www.eltiempo.com/justicia/cortes/amazonia-fue-declarada-sujeto-de-derechos-por-la-corte-suprema-201682>).

20 Les députés du Parlement européen ont adopté le 16 février 2017 un rapport sur l'évolution des règles de droit civil concernant la robotique qui suggère d'attribuer une « personnalité juridique spécifique aux robots » (*Proposition de résolution du Parlement européen contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique*, 2015/2103 (INL), en ligne : <http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_FR.html>, par. 59).

[8] Le droit canadien reconnait déjà des droits qui protègent les individus contre la discrimination en raison de leur appartenance à certains groupes (sexuels, religieux, ethniques, etc.)[21]. Enchâssés dans les Chartes des droits, ces « droits des minorités » sont considérés par la Cour suprême comme un des piliers de notre ordre constitutionnel[22]. Ces droits sont toutefois à distinguer des « droits collectifs » soit les droits qui appartiennent à un groupe *en tant que groupe*, et non à un groupe dans la mesure où celui-ci est constitué d'individus qui jouissent de ces droits. L'un des exemples de droit collectif au Canada est celui des droits ancestraux autochtones. Ces droits constitutionnels[23] sont détenus par les communautés autochtones elles-mêmes et ne peuvent, en principe, être exercés par les individus[24]. Le droit à l'autodétermination, qui appartient et est exercé par les peuples, est un autre exemple de droit collectif dévolu aux groupes *en tant que groupe*[25] .

I.3. QUEL TYPE DE DROIT À LA VIE PRIVÉE PEUT ÊTRE ATTRIBUÉ AUX « GROUPES » ?

[9] Afin d'éviter toute confusion, il importe de distinguer la vie privée des groupes *au sens faible* et la vie privée des groupes *au sens fort*[26]. La vie privée des groupes *au sens faible* réfère à la théorie de la vie privée relationnelle développée par Edward Bloustein dans les années 1970[27]. Cette forme de vie privée protège le désir et le besoin des individus de se rassembler, d'échanger de l'information, des émotions, de planifier et d'agir en commun dans l'atteinte de leurs objectifs[28]. Cette théorie conçoit la vie privée des groupes comme une extension de la vie privée individuelle[29]. Bloustein illustre sa théorie à l'aide de l'image du caucus dans le football américain[30]. Techniquement, seuls les joueurs à l'intérieur du caucus sont au courant de la stratégie. Bien que la stratégie discutée

21 *Charte canadienne des droits et libertés*, partie I de la *Loi constitutionnelle de 1982* [annexe B de la Loi de 1982 sur le Canada, 1982, c. 11 (R.-U), art. 15 (1) ; *Charte des droits et libertés de la personne,* RLRQ, c. C-12, art. 10.

22 Renvoi relatif à la sécession du Québec, [1998] 2 RCS 217, par. 32.

23 Loi constitutionnelle de 1982, préc. note 20, art. 35.

24 Behn c. Moulton Contracting Ltd., 2013 CSC 26, par. 30.

25 François Roch, « Réflexions sur l'évolution de la positivité du droit des peuples à disposer d'eux-mêmes en dehors des situations de décolonisation, » (2002) 15-1 *Revue québécoise de droit international* 33, p. 58.

26 Cette distinction imprègne les travaux de L. Floridi, préc. note 2, p. 90-91 et M. Loi et M. Christen, préc. note 11, p. 2.

27 Edward J. Bloustein, *Individual and Group Privacy*, New York, Transaction Publishers, 1978

28 *Id.*, p. 125.

29 *Id.*

30 *Id.*, p. 126.

en caucus puisse être partagée aux téléspectateurs par les analystes du match, cela ne vient pas amoindrir la vie privée relationnelle dans la mesure où la partie adverse n'a pas accès à cette information et ne peut anticiper le prochain jeu. Le « droit au caucus »[31] protège donc l'échange d'information au sein d'un groupe du regard extérieur d'un autre groupe antagoniste. Michele Loi et Markus Christen ont surnommé ce type de vie privée la "*What happens in Vegas stays in Vegas privacy*"[32] en référence aux agissements de certains touristes à Las Vegas qui ne souhaitent pas que leurs péripéties soient révélées à leurs conjointes.

[10] La vie privée des groupes *au sens fort* est une différente théorie qui postule qu'un groupe possède un droit collectif à la vie privée qui n'est pas réductible à la vie privée de chaque individu qui le compose. Luciano Floridi donne l'exemple de proches rassemblés pour les funérailles du défunt[33]. Les endeuillés forment un groupe actif qui partage une expectative de vie privée liée au besoin d'intimité, au respect du deuil et aux coutumes culturelles ou religieuses. Dans un tel contexte, il serait erroné de prétendre que chaque membre du groupe, c'est-à-dire chaque proche du défunt, bénéficie d'un droit *individuel* à des funérailles *privées*, il semble plus approprié d'admettre que nous sommes en présence d'un droit à la vie privée revendiqué par le groupe *en tant que groupe.*

[11] Certains auteurs sont d'avis que seuls les groupes actifs peuvent réalistement bénéficier d'un droit à la vie privée *au sens fort*[34]. À notre avis, si la vie privée des groupes se limite à protéger les groupes actifs — qui bénéficient déjà de protections juridiques[35] — alors cette théorie est de peu d'utilité puisqu'elle n'offre aucune protection aux groupes algorithmiques[36]. Il importe donc de développer l'argument voulant que ces groupes puissent également bénéficier d'un droit à la vie privée *au sens fort.*

31 *Id.*, p. 123 .

32 M. Loi et M. Christen, préc. note 11, p. 2.

33 L. Floridi, préc. note 12, p. 91.

34 L. Kammourieh et al., préc. note 10, p. 55 ; M. Loi et M. Christen, préc. note 11, p. 15.

35 Supra, section 1.2.

36 Au sujet des enjeux légaux entourant le profilage algorithmique voir Wim Schreurs, Mireille Hildebrandt, Els Kindt et Michaël Vanfleteren, « Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector », dans Mireille Hildebrandt et Serge Gutwirth (dir.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Dordrecht, Springer Netherlands, 2008, p. 241–270.

II. PROTÉGER LES GROUPES ALGORITHMIQUES : REDÉFINIR LE DROIT À LA VIE PRIVÉE

II.1. *MANTELERO* : LA DIMENSION COLLECTIVE DE LA PROTECTION DES DONNÉES

[12] Le *Median Equivalency Score* est une notation algorithmique créée par la firme Experian[37] qui cherche à prédire le risque de crédit des habitants d'une même région géographique sur la base de l'analyse de centaines de variables[38]. Les individus sont catégorisés non pas en fonction de leurs caractéristiques personnelles, mais plutôt selon la cote agrégée de leur milieu socio-économique. Du point de vue individuel, une personne peut n'avoir aucune réticence à ce que ses données personnelles soient collectées afin d'établir sa capacité d'emprunt, mais au niveau collectif, il demeure dans l'intérêt général d'une communauté de ne pas voir ses membres être stigmatisés comme de potentiels mauvais débiteurs sur la base d'une évaluation algorithmique potentiellement biaisée et discriminatoire[39]. Ces processus décisionnels, qui ne considèrent plus les individus pour ce qu'ils sont, mais selon la catégorie dont ils font partie bon gré mal gré, ont un impact significatif sur la vie des individus lorsqu'ils interviennent dans le domaine du crédit, mais également dans celui du logement, de l'assurance, de l'emploi, de la justice criminelle ou de la santé[40].

[13] Dans cette optique, Alessandro Mantelero soutient que la vie privée des groupes a pour fonction de protéger les intérêts collectifs non agrégés d'un groupe donné[41]. Ainsi, l'auteur soutient qu'il existe des priorités collectives en matière de protection de la vie privée notamment en ce qui concerne les risques de discrimination découlant du profilage

37 Experian, *Summarized Credit Statistics*, 2014, en ligne :<https://www.experian.com/small_business/pdf/fall03_catalog_summarized_credit.pdf>.

38 Voir le rapport de Pam Dixon et Robert Gellman,« The scoring of America: How secret consumer scores threaten your privacy and your future », *World Privacy Forum*, 2014.

39 La chercheuse Nikita Aggarwal souligne qu'un algorithme d'apprentissage automatique, entraîné à partir de données provenant d'une population à prédominance blanche peut donner lieu à des biais discriminatoires décourageant les prêts à l'égard des populations non blanches (Nikita Aggarwal, « Law and Autonomous Systems Series: Algorithmic Credit Scoring and the Regulation of Consumer Credit Markets », *Oxford Law Faculty*, 2018, en ligne : <https://www.law.ox.ac.uk/business-law-blog/blog/2018/11/law-and-autonomous-systems-series-algorithmic-credit-scoring-and>).

40 Au sujet des effets pervers des algorithmes de recommendation, voir Hannah Fry, Hello World: Being Human in the Age of Algorithms, 1st edition, New York, Norton & Company, 2018 et Cathy O'Neil, Weapons of math destruction: how big data increases inequality and threatens democracy, 1st edition, New York, Crown, 2016.

41 Des intérêts collectifs peuvent être partagés par l'ensemble d'un groupe sans qu'il y ait de divergence de points de vue entre ses membres (intérêts agrégés) ou avec des opinions contraires entre les membres (intérêts non agrégés) (Alessandro Mantelero, « Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection » (2016) 32-2 *Computer Law & Security Review* 238–255, p. 249) .

algorithmique[42]. Par conséquent, il décrit la vie privée des groupes comme le droit, pour un groupe, d'être protégé face aux préjudices potentiels pouvant être causés par un traitement invasif et discriminatoire des données[43].

[14] Cette conception propose d'élargir la portée « classique » du droit à la vie privée afin de tenir compte du fait que celui-ci constitue un garde-fou visant la protection d'intérêts sociétaux plus larges[44]. Cette approche rejoint celle du Commissaire à la vie privée du Canada (ci-après « CPVP ») qui définit la vie privée comme une condition préalable à l'exercice d'autres droits fondamentaux, notamment la liberté, l'égalité et la démocratie[45]. Cette conception élargie du droit à la vie privée évoque l'interprétation qui a été faite de l'article 8 de la *Convention européenne des droits de l'Homme* (ci-après « CEDH »)[46] dans une récente affaire mettant en cause le droit des générations à un environnement sain.

II.2. L'AFFAIRE URGENDA : UNE INTERPRÉTATION NOVATRICE DU DROIT À LA VIE PRIVÉE

[15] Le 9 octobre 2018, la Cour d'appel de La Haye a fait les manchettes en confirmant une ordonnance qui oblige l'État néerlandais à réduire ses émissions de GES d'au moins 25 % d'ici 2020 à la suite d'une procédure intentée par l'ONG de défense de l'environnement Urgenda[47]. L'ONG alléguait qu'en raison de son laxisme en matière de réduction des GES, le gouvernement manquait aux devoirs de diligence exprimés par les articles 2 (droit à la vie) et 8 (droit au respect de la vie privée et familiale) de la CEDH.

[16] Il importe de souligner deux aspects importants de cette décision. Premièrement, la Cour a reconnu à Urgenda l'intérêt juridique d'agir pour le compte de la génération actuelle et des générations futures de Néerlandais qui devront faire face aux effets négatifs du changement

42 Soulignons que le CPVP considère que le profilage algorithmique des individus donnant lieu à un « traitement injuste, contraire à l'éthique ou discriminatoire » constitue une pratique inacceptable au sens du par. 5 (3) de la *Loi sur la protection des renseignements personnels et les documents électroniques*.

43 A. Mantelero, préc. note 41, p. 246.

44 "Privacy has long been known to safeguard societal interests broader than privacy interest" (Ignacio N. Cofone, « Antidiscriminatory Privacy » (2019) 72 *SMU L. Rev*. 139, 147).

45 Commissariat à la protection de la vie privée du Canada, Rapport annuel au Parlement 2018-2019 concernant la Loi sur la protection des renseignements personnels et la Loi sur la protection des renseignements personnels et les documents électroniques, 2019, Gatineau, en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/201819/ar_201819/>.

46 Convention de sauvegarde des droits de l'Homme et des libertés fondamentales, STCE n° 005.

47 ECLI:NL:GHDHA:2018:2610, 9 octobre 2018, en ligne : <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHDHA:2018:2610>.

climatique au cours de leur vie si les émissions mondiales de GES ne sont pas réduites[48]. Deuxièmement, la Cour affirme que les changements climatiques constituent une réelle menace qui risque de profondément perturber notre mode de vie et que par conséquent, l'État néerlandais doit réduire ses émissions de GES afin de se conformer à son devoir de diligence envers le bien-être de ses citoyens présents et futurs[49].

[17] L'affaire *Urgenda* illustre comment un droit collectif à la vie privée peut concrètement bénéficier aux groupes. D'une part, la décision reconnait que des groupes dont la composition est instable (les générations présentes et futures) peuvent faire valoir leur intérêt collectif d'être protégé face à un préjudice potentiel et hypothétique (les conséquences du réchauffement climatique). De l'autre, elle propose une interprétation novatrice des droits fondamentaux qui tient compte de l'impact des changements climatiques sur le collectif et non seulement sur l'individu afin de déterminer si un droit reconnu par la CEDH est violé et si les États doivent prendre action.

[18] Cette approche permet d'entrevoir la possibilité pour les groupes algorithmiques de bénéficier également d'un droit à la vie privée *au sens fort*. En effet, la composition abstraite du groupe ne devrait pas l'empêcher de faire valoir son intérêt réel d'être protégé contre un préjudice potentiel. Ainsi, même si les groupes algorithmiques sont en constante mutation, les risques que leurs membres soient victimes d'atteintes à la vie privée et de discrimination à la suite du traitement algorithmique des données demeurent. Le devoir de diligence de l'État à l'égard de ses citoyens milite en faveur de l'adoption de mesures concrètes permettant de les protéger adéquatement. La prochaine section s'y attarde.

II.3. *COFONE* : LA VIE PRIVÉE ANTIDISCRIMINATOIRE

[19] La théorie de la vie privée antidiscriminatoire, développée par Ignacio Cofone, soutient que les règles en matière de protection de la vie privée peuvent servir à lutter efficacement contre la discrimination lorsqu'elles limitent l'accès aux renseignements que les lois en matière de non-discrimination considèrent être dommageables dans le cadre d'un

48 *Id.*, par. 34 à 38.

49 *Id.*, par. 73.

processus décisionnel[50]. Cofone part du constat que le droit à l'égalité intervient généralement *ex post*, c'est-à-dire après le préjudice causé par un acte discriminatoire. Or, comme il vaut mieux prévenir que guérir, l'auteur propose d'empêcher l'*acquisition*, par le décideur, de données sensibles[51] plutôt que de contrer l'*utilisation* discriminatoire de ces données[52].

[20] Des recherches ont toutefois mis en lumière que des décisions prises sur la base d'un traitement algorithmique peuvent être discriminatoires même lorsque toutes les données sensibles ont été retirées d'un ensemble de données[53]. En effet, les algorithmes d'apprentissage automatique peuvent tirer des inférences à partir de certaines données qui agissent comme intermédiaires (*proxy*) pour *révéler* une caractéristique protégée par les lois anti-discrimination. Ainsi, le code postal peut servir d'intermédiaire à une discrimination raciale[54] et les « J'aime » d'un profil Facebook peuvent révéler l'appartenance religieuse, les convictions politiques, l'orientation sexuelle d'une personne[55]. Par conséquent, Cofone souligne que la vie privée antidiscriminatoire passe également par le fait d'identifier et de bloquer les données servant d'intermédiaires[56].

[21] Or, il s'avère pratiquement impossible de bloquer toutes les données pouvant servir d'intermédiaires à des données sensibles, car les algorithmes d'apprentissage automatique seront toujours en mesure de tirer de *nouvelles* corrélations entre les données à leur disposition[57]. De plus, un renseignement qui agit comme intermédiaire pour une caractéristique protégée peut également être révélateur d'information utile et légitime. Par exemple, le niveau d'éducation peut être utilisé

50 I. Cofone, préc. note 45, et Ignacio N. Cofone, « Algorithmic Discrimination Is an Information Problem » (2019) 70-6 *Hastings LJ* 1389.

51 Nous utilisons le terme « donnée sensible » pour désigner tout renseignement portant sur l'un des motifs de non-discrimination prévu à l'article 10 de la *Charte des droits et libertés de la personne*, préc. note 21.

52 I. Cofone, préc. note 45, p. 140

53 Solon Barocas et Andrew D. Selbst, « *Big Data's Disparate Impact* », (2016) 104 *Calif. L. Rev.* 671, 675

54 Le "redlining" décrit le fait que les données géographiques sont profondément liées aux pratiques historiques d'exclusion et de discrimination raciales (Maya Sen et Omar Wasow. "Race as a Bundle of Sticks: Designs that Estimate Effects of Seemingly Immutable Characteristics." » (2016) 19 *Annual Review of Political Science* 499-522).

55 Il est possible d'inférer certains attributs personnels comme le genre, l'âge, la race, l'appartenance religieuse, les convictions politiques, la consommation de drogues et d'alcool, l'orientation sexuelle et le statut conjugal à partir de l'analyse de 58 000 « J'aime » sur Facebook (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.)

56 I. Cofone, préc. note 45, p. 172.

57 I. Cofone, préc. note 50, p. 1414.

comme intermédiaire pour prédire la race d'un individu, mais il peut aussi renseigner sur la performance au travail.

[22] Une autre approche consiste à confier la collecte et la gestion des données sensibles à un tiers de confiance[58]. Une organisation, qui souhaite développer un algorithme de recommandation, ne devrait avoir accès qu'aux données non sensibles nécessaires à l'accomplissement de sa tâche. En parallèle, une organisation tierce peut être chargée de collecter les données sensibles des individus dont les données (non sensibles) servent à l'entrainement de l'algorithme. Doté d'un accès à l'algorithme de l'organisation, le tiers de confiance peut ensuite recouper les résultats de celui-ci avec les données sensibles des individus afin de détecter la présence de biais discriminatoires. Un assureur pourrait par exemple développer un algorithme de recommandation pour l'aider à déterminer les primes de ses clients. Après s'être procuré une nouvelle police d'assurance sur le site web de l'assureur, le client serait alors dirigé vers le domaine d'un organisme de protection des consommateurs où il lui serait demandé de fournir certaines données sensibles afin de s'assurer que la prime générée par l'algorithme de l'assureur n'est pas discriminatoire.

CONCLUSION

[23] Les mégadonnées instaurent un nouveau « régime de vérité »[59] qui conduit les organisations à juger les individus non plus en fonction de leurs caractéristiques propres, mais selon leur appartenance à une segmentation artificielle de la société. Bien que la vie privée des groupes demeure une théorie inachevée, celle-ci nous invite à une réflexion cruciale à la lumière des récents développements technologiques. Le paradigme juridique axé sur les droits individuels apparait de plus en plus dépassé face aux conséquences du profilage algorithmique à l'échelle collective. Le temps semble être venu d'adopter une conception élargie du droit à la vie privée comme condition préalable à la protection et à l'exercice d'autres droits fondamentaux. Cette redéfinition permettrait de protéger les groupes *en tant que groupe* et de reconnaître leur intérêt collectif à ne pas être victime de discrimination basée sur des biais dans le traitement algorithmique des données.

58 Michael Veale and Reuben Binns, « Fairer Machine Learning in the Real World: Mitigating Discrimination Without Collecting Sensitive Data » (2017) 4 *Big Data & Society* 2.

59 A. Rouvroy, préc. note 6, page 9.