Commission des droits de la personne et des droits de la jeunesse Québec

CI-138
2021-02-02
S. Mekki

Cat. 2.412.42.8

MÉMOIRE À LA COMMISSION DES INSTITUTIONS DE L'ASSEMBLÉE NATIONALE

PROJET DE LOI N^{O} 64,

LOI MODERNISANT LES DISPOSITIONS LÉGISLATIVES EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

Octobre 2020

Document adopté à la 685e séance de la Commission,
tenue le 16 octobre 2020, par sa résolution COM- 685-4.1.2

Jean-François Trudel
Secrétaire de la Commission

Analyse, recherche et rédaction :

Me Anastasia Berwald, conseillère juridique
Me Marie Carpentier, conseillère juridique
Mathieu Forcier, chercheur
Direction de la recherche

Collaboration à la recherche :

Guillaume Rioux, stagiaire
Direction de la recherche

Traitement de texte :

Sylvie Durand
Direction de la recherche

TABLE DES MATIÈRES

INTRODUCTION

La Commission des droits de la personne et des droits de la jeunesse[1] assure le respect et la promotion des principes énoncés dans la *Charte des droits et libertés de la personne* du Québec[2]. Elle assure aussi la protection de l'intérêt de l'enfant, ainsi que le respect et la promotion des droits qui lui sont reconnus par la *Loi sur la protection de la jeunesse*[3]. Elle veille également à l'application de la *Loi sur l'accès à l'égalité en emploi dans des organismes publics*[4].

Pour ce faire, la Commission, dont les membres sont nommés par l'Assemblée nationale[5], a entre autres le mandat de « relever les dispositions des lois du Québec qui seraient contraires à la Charte et faire au gouvernement les recommandations appropriées »[6]. C'est en vertu de cette responsabilité que la Commission a analysé le projet de loi nº 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*[7].

L'objet du projet de loi nº 64 est de « modernise [r] l'encadrement applicable à la protection des renseignements personnels dans diverses lois, dont la Loi sur l'accès aux documents des organismes publics et la Loi sur la protection des renseignements personnels dans le secteur privé »[8]. Il s'agit d'une réforme substantielle et attendue de longue date du régime de protection des renseignements personnels instauré dans les années 1980. En raison d'un délai trop court, la Commission a décliné l'invitation à participer aux consultations particulières et auditions publiques qui ont eu lieu du 22 au 29 septembre 2020.

---

1 Ci-après « Commission ».

2 *Charte des droits et libertés de la personne*, RLRQ, c. C-12 (ci-après « Charte »).

3 *Loi sur la protection de la jeunesse*, RLRQ, c. P-34.1.

4 *Loi sur l'accès à l'égalité en emploi dans des organismes publics*, RLRQ, c. A-2.01.

5 *Id.*, art. 58 al. 2.

6 *Id.*, art. 71 al. 1 et al. 2 (6).

7 *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, projet de loi nº 64, (présentation – 12 juin 2020), 1re sess., 42e légis. (Qc), « Notes explicatives » (ci-après « projet de loi nº 64 »).

8 *Id.*, « Notes explicatives ».

La Commission aimerait d'ailleurs exprimer sa préoccupation pour le peu de temps qui est consacré à l'étude de ce projet de loi et le court délai qui a été accordé aux intervenants entre le moment de leur convocation et la date prévue de leur comparution, compte tenu, notamment, de l'ampleur de ce projet. L'importance des enjeux qui y sont abordés aurait commandé, de l'avis de la Commission, des consultations générales plutôt que des consultations particulières. Elle a d'ailleurs déjà mentionné la nécessité d'un débat démocratique et transparent à d'autres occasions où le droit au respect de sa vie privée[9], garanti par la Charte, était mis en cause[10].

Le présent mémoire est, parmi les mémoires que la Commission a adoptés en 2020, le quatrième à traiter, entre autres, de la question du droit au respect de sa vie privée. Cette question a notamment été abordée dans le cadre de l'étude du projet de loi nº 53[11], puis dans le contexte des consultations menées par la Commission d'accès à l'information[12] sur l'encadrement de l'intelligence artificielle[13]. Plus récemment, la Commission s'est penchée sur les applications de notification de contacts[14]. C'est dire l'intérêt que porte la Commmission aux enjeux qui entourent le respect de ce droit fondamental et qui mettent en cause d'autres droits et libertés de la personne.

Nous proposons ici une analyse en trois parties. La première porte sur la valeur des renseignements personnels dans le contexte social actuel. La seconde s'intéresse aux droits de la Charte en cause dans la collecte et l'utilisation des renseignements personnels, l'utilisation

---

9 Charte, art. 5.

10 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Mémoire à la Commission de la santé et des services sociaux, Projet de loi nº 59, Loi concernant le partage de certains renseignements de santé*, (Cat. 2.412.67.9), 2012, p. 8 [En ligne]. https://cdpdj.qc.ca/storage/app/media/publications/memoire_PL_59_renseignements_sante.pdf

11 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Mémoire à la Commission des finances publiques sur le projet de loi nº 53, Loi sur les agents d'évaluation de crédit*, (Cat. 2.412.132), 2020, [En ligne]. https://cdpdj.qc.ca/storage/app/media/publications/memoire_PL53_agence_evaluation_credit.pdf

12 Ci-après « CAI ».

13 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Mémoire à la Commission d'accès à l'information sur le document de consultation « Intelligence artificielle* », (Cat. 2.412.133), 2020, [En ligne]. https://cdpdj.qc.ca/storage/app/media/publications/memoire_consultation_CAI_IA.pdf

14 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Mémoire à la Commission des institutions de l'Assemblée nationale au sujet d'outils technologiques de notification des contacts ainsi que sur la pertinence de ce type d'outils, leur utilité et le cas échéant, les conditions de leur acceptabilité sociale dans le cadre de la lutte contre la COVID-19*, (Cat. 2.412.135), 2020 [En ligne]. https://cdpdj.qc.ca/fr/publications/memoire_consultation_outils_notification_covid-19

étant ici entendue comme comprenant le traitement, la communication, la conservation ou la destruction des renseignements personnels. Enfin, la dernière partie présente une analyse du projet de loi au regard des droits en cause.

1 LA VALEUR DES RENSEIGNEMENTS PERSONNELS DANS LE CONTEXTE SOCIAL ACTUEL

L'évolution de l'environnement sociotechnique commande un renforcement des protections du droit au respect de sa vie privée[15] et des autres droits qui sont affectés par la collecte et l'utilisation des renseignements personnels. Nous situons ici l'analyse de la réforme législative en matière de protection des renseignements personnels dans le contexte social où les données personnelles sont une ressource de plus en plus centrale aux régimes de surveillance[16] d'acteurs publics et privés. Dans cette section, nous traiterons de l'érosion de la frontière entre les domaines publics et privés avec les nouvelles technologies, de la centralité des données dans le système économique contemporain et des inégalités systémiques qui conditionnent l'exercice du droit au respect de sa vie privée. Nous aborderons à ce sujet les enjeux relatifs à la surveillance policière et à la surveillance en milieu de travail de même que les aspects genrés de la vie privée et la vie privée des mineurs.

Soulignons que la pandémie de COVID-19 a stimulé la réflexion sur la collecte de données et les conséquences de l'utilisation de nouvelles technologies basées sur les données en matière de droits et libertés. Cette pandémie vient avec son lot de nouvelles réalités et de risques d'exposition à des pratiques de surveillance ou à des failles de sécurité des données. Par exemple, dans le but de limiter la propagation du virus, des États et des employeurs ont eu recours à des technologies qui collectent et traitent des données et qui sont susceptibles de porter atteinte aux droits et libertés[17]. Durant la pandémie, des services publics, notamment

---

15 Charte, art. 5.

16 Voir *infra* section 1.1.

17 Voir Dave GERSHGORN, « We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World », 9 avril 2020, [En ligne]. https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9 ; Natalie CHYI, « The Workplace-Surveillance Technology Boom », *Slate* (12 mai 2020), [En ligne]. https://slate.com/technology/2020/05/workplace-surveillance-apps-coronavirus.html; James VINCENT, « Amazon deploys AI 'distance assistants' to notify

dans les domaines de l'éducation et des services de santé, ont été offerts en ligne, ce qui implique des enjeux de sécurité des renseignements personnels et une exposition accrue à la collecte de données[18]. Il en va de même de la généralisation du télétravail dans certains milieux[19]. Nous y reviendrons.

1.1 L'érosion de la frontière entre les domaines publics et privés

Qu'elle soit le fait de l'État ou d'acteurs privés[20], la surveillance par la collecte et l'utilisation des données numériques est facilitée par l'érosion de la frontière entre les domaines publics et privés. En 2015, alors qu'elle commentait le rapport quinquennal de la CAI, la Commission indiquait :

> [L] a Commission est préoccupée de la distinction, maintenue […] entre le traitement réservé aux informations détenues par le secteur public et celui réservé aux informations détenues par le secteur privé. Il appert pourtant que les autorités publiques de pays partout dans le monde requièrent de plus en plus souvent l'accès systématique aux informations détenues par des entités privées. Des orientations gouvernementales promouvant entre autres le droit au respect de la vie privée et le droit à l'information ne peuvent faire l'économie d'une prise en compte de l'érosion de la séparation traditionnelle entre les secteurs, et de la porosité entre le domaine public et le domaine privé en ce qui a trait à l'accessibilité et à l'utilisation des données recueillies.[21]

---

warehouse workers if they get too close », *The Verge* (16 juin 2020), [En ligne]. https://www.theverge.com/2020/6/16/21292669/social-distancing-amazon-ai-assistant-warehouses-covid-19

18 Voir notamment COMMISSION D'ACCÈS À L'INFORMATION, « Outils d'enseignement à distance », 1er mai 2020, [En ligne]. https://www.cai.gouv.qc.ca/covid-19-questions-frequentes/outils-denseignement-a-distance/; Marco LAVERDIÈRE, « La télésanté après la pandémie : Quelques difficultés et questions à régler », Chaire de recherche du Canada sur la culture collaborative en droit et politiques de la santé », 17 avril 2020, [En ligne]. https://www.chairesante.ca/articles/2020/la-telesante-apres-la-pandemie-quelques-difficultes-et-questions-a-regler/

19 COMMISSION D'ACCÈS À L'INFORMATION, « Sécurité de l'information et télétravail : employé », 1er mai 2020, [En ligne]. https://www.cai.gouv.qc.ca/covid-19-questions-frequentes/securite-de-linformation-et-teletravail-employe/

20 Notons que la surveillance n'est pas limitée aux acteurs étatiques et commerciaux, mais comprend aussi à la surveillance interpersonnelle. Voir Daniel TROTTIER, « Interpersonal Surveillance on Social Media », (2012) 37 :2, *Canadian Journal of Communication*, p. 319-332, [En ligne]. https://www.cjc-online.ca/index.php/journal/article/view/2536/2315

21 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Mémoire à la commission des institutions de l'Assemblée nationale commentaires sur le 6e rapport quinquennal de la Commission d'accès à l'information intitulé « Rétablir l'équilibre – Rapport sur l'application de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et de la loi sur la protection des renseignements personnels dans le secteur privé »,* (Cat. 2.412.42.7), 2017, p. 5, [En ligne]. https://cdpdj.qc.ca/storage/app/media/publications/memoire_acces_information.pdf, citant Fred H. CATE, James X. DEMPSEY et Ira S. RUBINSTEIN, « Systematic gouvernment access to private-sector data », (2012) 2:4 *International Data Privacy Law* 195, p. 195 et *Le droit à la vie privée à l'ère du numérique*, Rapport du

Des auteurs notent, entre autres, un déficit de transparence, de contrôle et de balises quant à l'usage des données dans les relations étroites entre le secteur privé et les services de police[22]. Nous y reviendrons.

Par ailleurs, le développement des nouvelles technologies contribue à rendre toujours plus floue la séparation entre les sphères de la vie privée et de la vie publique[23]. Selon le professeur de droit Joel R. Reidenberg, la technologie a ainsi permis la création du « citoyen transparent », c'est-à-dire un citoyen dont l'identité et les renseignements personnels sont désormais exposés publiquement et disponibles pour la surveillance et l'exploration (*data-mining*) par les acteurs étatiques et privés[24]. Cette transparence des citoyens facilite notamment l'utilisation par les pouvoirs publics de renseignements sans avoir à se soumettre aux mécanismes de contrôle politiques et légaux traditionnels, tels que ceux offerts par la Charte ou la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[25].

Le web et les médias sociaux sont des espaces où les distinctions entre ce qui relève de la vie privée et de la vie publique sont particulièrement floues et poreuses[26]. Ils ont souvent été présentés comme étant parties prenantes d'une nouvelle sphère publique et ils sont aujourd'hui un lieu privilégié d'actions et d'expressions de nature politiques[27]. Il s'agit aussi d'espaces

---

Haut-Commissariat des Nations Unies aux droits de l'homme, Doc. N.U. A/HRC/27/37, 2014, par 27 et réitéré dans COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 13, p. 20.

22 Kate ROBERTSON, Cynthia KHOO et Yolanda SONG, *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada*, Citizen Lab, University of Toronto, 1er septembre 2020, p. 90-93. [En ligne]. https://citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/

23 Daniel TROTTIER et Christian FUCHS, « Theorising Social Media, Politics and the State: An Introduction » dans D. TROTTIER et C. FUCHS (dir.), *Social Media, Politics and the State: Protests, Revolutions, Riots, Crime and Policing in the Age of Facebook, Twitter and Youtube*, New York, Routledge, 2014, p. 3-38; Katharine SARIKAKIS et Lisa WINTER, « Social Media Users' Legal Consciousness About Privacy », *Social Media + Society*, Janvier-mars, 2014, p. 1-14, [En ligne]. https://journals.sagepub.com/doi/pdf/10.1177/2056305117695325

24 Joel R. REIDENBERG, « The Transparent Citizen », (2015) 42:7 *Loyola University Chicago Law Journal* 437.

25 RLRQ, c. A-2.1 (ci-après « Loi sur le public »).

26 Zizi PAPACHARISSI, *Affective Publics. Sentiments, Technology, and Politics*, 2015, Oxford, Oxford University Press

27 Voir notamment Z. PAPACHARISSI, *id.*; Shelley BOULIANNE, « Social media use and participation : a meta-analysis of current research » (2015) 18:5 *Information, Communication & Society* 524; Majid KHOSRAVINIK, « Social Media Techno-Discursive Design, Affective Communication and Contemporary Politics » (2018) 11 *Fundan Journal of the Humanities and Social Sciences* 427; Nikita CARNEY, « All Lives Matter, but so Does Race: Black Lives Matter and the Evolving Role of Social Media » (2016) 40:2 *Humanity & Society* 180.

utilisés pour le développement d'interactions plus ou moins intimes et pour la présentation de soi, notamment chez les jeunes[28]. Or, comme nous le verrons plus loin, ces plateformes appartiennent ultimement à des entreprises privées intéressées à maximiser leurs profits sur la base de l'exploitation des données produites par les utilisateurs.

À titre d'exemple, sur une plateforme comme Facebook, les perceptions de la démarcation entre ces sphères varient selon les personnes, le contexte d'utilisation et le type d'information[29]. Il apparaît aussi que les usagers considèrent que les données sur leurs opinions, associations et émotions constituent des renseignements personnels qui devraient être protégés par le droit à la vie privée[30].

La littérature montre en effet que les individus affirment accorder une grande importance au droit au respect de leur vie privée et au contrôle quant à la collecte et à l'utilisation de leurs renseignements personnels, et ce, tout en exprimant un sentiment d'impuissance ou une résignation quant à la protection effective de leurs données en lien avec les nouvelles technologies[31]. À ce propos, selon un récent sondage du Commissariat à la protection de la vie

---

28 Lisa M. KRUSE, Dawn R. NORRIS et Jonathan R. FLINCHUM, « Social Media as a Public Sphere? Politics on Social Media », (2018) 59:1 *The Sociological Quaterly* 62; Monica Anderson et Jingjing Jiang, « Teens' Social Media Habits and Experiences », *Pew Research Center*, 28 novembre 2018, [En ligne]. https://www.pewresearch.org/internet/2018/11/28/teens-social-media-habits-and-experiences/

29 Voir notamment, Jacquelyn BURKELL, Alexandre FORTIER, Lorraine WONG et Jennifer LYNN SIMPSON, « Facebook: public space, or private space? »(2014) 17 :8 *Information, Communication & Society* 974; Annette MARKHAM et Simona STAVROVA, « Internet/Digital Research », dans David SILVERMAN (dir.), *Qualitative Research*, 4e éd., Londres : SAGE, 2016, p. 229

30 K. SARIKAKIS et L. WINTER, préc., note 23.

31 *Id.;* Siobhan LYONS, « You may be sick of worrying about online privacy, but "surveillance apathy" is also a problem », *The Conversation*, 7 novembre 2017, [En ligne]. https://theconversation.com/you-may-be-sick-of-worrying-about-online-privacy-but-surveillance-apathy-is-also-a-problem-86474; Marry MADDEN et Lee RAINE, « Americans' Attitudes About Privacy, Security and Surveillance », Pew Research Center, 20 mai 2015, [En ligne]. https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/; Cette situation toucherait les jeunes de façon plus aiguë. Même s'ils sont conscients des risques associés au partage de renseignements en ligne et qu'ils souhaitent protéger leur vie privée, ils tendent à se résigner à ce déficit de contrôle, ce qui ne les empêche pas d'adopter des comportements de protection de la vie privée en ligne. Voir notamment K. SARIKAKIS et L. WINTER, préc., note 23; Eszter HARGITTAI et Alice MARWICK, « "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy » (2016) 10 *International Journal of Communication* 3737, [En ligne]. https://ijoc.org/index.php/ijoc/article/view/4655/1738. Le paradoxe entre les préoccupations pour le respect de la vie privée et le partage de renseignements personnels est également valable pour des données sensibles comme celles produites par les appareils intelligents à porter sur soit tels que les moniteurs d'activité physique. Voir notamment Jessica VITAK, Yuting LIAO, Priya KUMAR, Michael ZIMMER et Katherine KRITIKOS, « Privacy Attitudes and Data Valuation Among Fitness Tracker Users », dans *Transforming Digital Worlds*, 2018, p. 229, [En ligne]. https://pearl.umd.edu/wp-content/uploads/2017/08/Vitak_etal-2018-iconf-fitbit-privacy.pdf;

du Canada, les Canadiens sont préoccupés de leur vie privée en ligne et souhaitent exercer un meilleur contrôle sur leurs renseignements personnels, notamment à l'égard des entreprises[32]. Or, ces aspirations sont mises à mal par les dynamiques de marchandisation des renseignements personnels.

1.2 Les données et leur valeur marchande

La Commission a récemment exprimé ses inquiétudes quant aux impacts de l'exploitation des données numériques à des fins commerciales sur l'exercice des droits et libertés[33]. Les renseignements personnels et les métadonnées[34] générées par les personnes sont en effet des ressources importantes dans le système économique contemporain[35].

La sociologue et professeure émérite de la Harvard School of Business Shoshana Zuboff parle alors d'un capitalisme de surveillance[36]. Il est question ici d'un système économique où les comportements humains font office de données brutes que des entreprises privées exploitent gratuitement par la collecte, la vente et la prédiction de comportements[37].

Toutes les activités en ligne, peu importe leur nature, sont autant de renseignements d'intérêt susceptibles d'être monétisés. Il peut s'agir de ce qu'une personne achète, ce qu'elle

---

32 Par exemple, 55 % se disent préoccupés et 32 % quelque peu préoccupés par le fait que des plateformes des médias sociaux recueillent leurs renseignements personnels afin de créer un profil détaillé. De plus, 86 % des répondants estiment qu'il ne devrait pas être possible pour les entreprises de partager leurs renseignements à des fins autres que le service fourni. En ce qui concerne l'utilisation de ces renseignements pour voler leur identité, 62 % se disent préoccupés et 28 % quelque peu préoccupés. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Sondage auprès des Canadiens sur la protection de la vie privée de 2018-2019 », 9 mai 2019, [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/2019/por_2019_ca/#fig03

33 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 14; COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 13

34 Une métadonnée est une donnée qui fournit des renseignements sur une autre donnée : « Il s'agit en fait de renseignements qui sont générés lorsqu'on utilise la technologie et qui permettent de situer dans leur contexte (qui, quoi, où, quand et comment) diverses activités. » COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Métadonnées et vie privée. Un aperçu technique et juridique*, octobre 2014, [En ligne]. https://www.priv.gc.ca/media/1793/md_201410_f.pdf, p. 1.

35 Shoshana ZUBOFF, *The Age of Surveillance Capitalism*, New York, Public Affairs, 2019.

36 *Id.*

37 La monétisation des comportements en ligne a été créée chez Google après l'éclatement de la bulle Internet au tournant du millénaire et est depuis devenue un mécanisme central des opérations commerciales.

recherche, ce qu'elle consulte et durant combien de temps, ce sur quoi elle clique, ses déplacements, ses images, les mouvements de son curseur, le ton de sa voix, etc[38]. Ces informations sont monétisées par le biais de courtiers en données, c'est-à-dire « des entreprises qui recueillent des renseignements personnels sur les consommateurs auprès de diverses sources publiques et non publiques et les revendent à d'autres entreprises »[39]. La forme la plus connue d'exploitation commerciale des données est celle de la publicité ciblée. Des usagers sont exposés à des produits différents en fonction de leurs comportements et de leur appartenance à un groupe sociodémographique particulier, le tout calculé par des algorithmes qui traitent des données massives dans le but de maximiser le rendement en offrant un certain type de publicité à un moment à une certaine personne[40].

Notons que cela s'opère généralement sans que les détenteurs des renseignements personnels soient conscients des activités commerciales par lesquelles transitent leurs données[41]. Comme le note à cet effet le Commissariat à la protection de la vie privée du Canada, ces activités rendent les intéressés « impuissants » et « vulnérables en les empêchant d'exercer un contrôle sur leurs renseignements personnels ».[42]

Qui plus est, dans les dernières années, on a observé un nombre croissant de sources de données et une diversification des types de données collectées, incluant des données biométriques[43]. Pensons aux voitures automatisées, aux drones, aux systèmes de

---

38 Louise MATSAKIS, « The WIRED Guide to Your Personal Data (and Who Is Using It) », *Wired*, 15 février 2019, [En Ligne]. https://www.wired.com/story/wired-guide-personal-data-collection/

39 FEDERAL TRADE COMMISSION, citée dans COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Les courtiers en données. Regards sur les paysages canadiens et américains*, septembre 2014, p. 2, [En Ligne]. https://www.priv.gc.ca/media/1779/db_201409_f.pdf

40 En analysant les données d'activités des utilisateurs, il serait également possible de prédire l'arrivée d'un certain volume de consommateurs à un endroit et à une heure précise. Voir. S. ZUBOFF, préc., note 35.

41 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 39. Voir également Yael GRAUER, « What Are 'Data Brokers,' and Why Are They Scooping Up Information About You? », *Vice*, 27 mars 2018, [En ligne]. https://www.vice.com/en/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection

42 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *id.*

43 Voir Amba KAK (dir.), *Regulating Biometrics. Global Approaches and Urgent Questions*, AI Now, 2020, [En ligne]. https://ainowinstitute.org/regulatingbiometrics.pdf

reconnaissance faciale, aux technologies de la « maison intelligente » ou encore à l'industrie de la surveillance axée sur la santé avec les appareils intelligents à porter sur soi[44].

Comme le note Zuboff, alors que nous avons tendance à penser que nous utilisons en ligne des plateformes et services gratuits, nous faisons plutôt office de ressources au sein d'une chaîne d'approvisionnement pour la production de prédictions de comportements calculées sur la base de nos comportements passés et présents : « Ils nous qualifient d'utilisateurs, mais, en réalité, ils nous utilisent comme matière première brute pour leurs processus de production. »[45] [Notre traduction.]

Les entreprises de l'industrie des technologies de l'information ne se limitent pas à la surveillance des comportements des personnes en ligne. L'agrégation et le traitement automatisé des métadonnées visent ultimement à influencer le comportement des personnes et des communautés de façon à maximiser la consommation de produits et services et la profitabilité des entreprises financièrement impliquées, que ce soit par la collecte, le traitement ou l'achat de données. Les données produites sont des ressources utilisées afin d'ajuster et d'influencer les comportements, au bénéfice des entreprises.

Ce conditionnement du comportement se fait notamment par le biais de « coups de coude numériques » (*digital nudging*), par exemple en insérant un contenu ciblé dans le fil de nouvelles Facebook d'une personne ou en insérant un bouton « acheter » au moment opportun[46]. Le capitalisme de surveillance n'encouragerait donc pas seulement des pratiques attentatoires au droit à la vie privée, mais il engendrerait également des dynamiques qui restreignent l'autonomie et l'agentivité humaines et, conséquemment, l'exercice des droits démocratiques[47]. Les auteurs d'une étude sur la publicité ciblée en fonction des caractéristiques

---

44 Nous reviendrons sur les appareils intelligents à porter sur soi à la section 3.2 sur la notion de renseignement sensible.

45 Citée dans Zachary MACK, « Shoshana ZUBOFF on surveillance capitalism », *The Verge*, 26 mars 2019, [En Ligne]. https://www.theverge.com/2019/3/26/18282360/age-of-surveillance-capitalism-shoshana-zuboff-data-collection-economy-privacy-interview-vergecast

46 S. ZUBOFF, préc., note 35.

47 Shoshana ZUBOFF, « Surveillance Capitalism and the Challenge of Collective Action », (2019) 28-1 *New Labor Forum* 10-29, DOI : 10.1177/1095796018819461.; Soshana Zuboff, « You Are Now Remotely Controlled », *The New York Times*, 24 janvier 2020, [En Ligne]. https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html

psychologiques basées sur les empreintes numériques des personnes sur les médias sociaux concluent qu'il est ainsi possible d'« altérer significativement le comportement » d'individus et d'« influencer le comportement de larges groupes de personnes en adaptant les appels persuasifs aux besoins psychologiques des publics cibles »[48] [notre traduction].

Ce type de pratiques fait écho, dans la sphère politique, au scandale Facebook-Cambridge Analytica dans lequel les données personnelles de 87 millions d'utilisateurs ont été collectées et utilisées sans leur consentement pour influencer le vote des électeurs, principalement dans le cadre des élections présidentielles états-uniennes de 2016[49]. Pour ce faire, Cambridge Analytica a effectué un profilage psychométrique et politique sur la base de sondages en ligne et de données recueillies sur Facebook pour ensuite développer des algorithmes en mesure de cibler des électeurs avec des publicités politiques hautement personnalisées et modifier leur comportement en faveur d'acteurs politiques financièrement impliqués dans l'opération[50].

Michael Veale, chercheur en régulation et droits numériques, note que l'analyse des données à des fins marchandes est de plus en plus sophistiquée avec le développement d'outils cryptographiques qui se veulent respectueux de la vie privée, mais qui ne permettent pas moins de surveiller et de modifier les comportements :

> Ces outils confèrent à ceux qui contrôlent et coordonnent des millions et même des milliards d'ordinateurs le pouvoir monopolistique d'analyser et de façonner des communautés et des pays ou même de modifier le comportement individuel, comme le ciblage confidentiel des publicités basé sur les données les plus sensibles – le tout sans que les données d'un individu n'aient quitté son téléphone[51]. [Notre traduction.]

---

48 S. C. MATZ, M. KOSINSKI, G. NAVE et D. J. STILLWELL, « Psychological targeting as an effective approach to digital mass persuasion », (2017) 114-48 *Proc. Natl. Acad. Sci.* 12714-12719, 12714, DOI : 10.1073/pnas.1710966114.

49 Jim ISAAK and Mina J. HANNA, « User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection », (2018) 51:8 Computer 56 à la p. 57 doi: 10.1109/MC.2018.3191268; S. ZUBOFF, « You Are Now Remotely Controlled », préc., note 47.

50 Voir Alex HERN, « Cambridge Analytica: how did it turn clicks into votes? », *The Guardian*, 6 mai 2018, [En ligne]. https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie

51 Michael VEALE, « Privacy is not the problem with the Apple-Google contact-tracing toolkit », *The Guardian*, 1 er juillet 2020, [En ligne]. https://www.theguardian.com/commentisfree/2020/jul/01/apple-google-contacttracing-app-tech-giant-digital-rights?CMP=share_btn_tw.

Pour des entreprises de l'industrie technologique, la crise sanitaire est une nouvelle occasion d'étendre leurs chaînes d'approvisionnement en données[52]. L'industrie de la technologie peut proposer des « solutions » technologiques qui impliquent de l'intelligence artificielle et donc encore davantage de collecte et de traitement automatisé de données, notamment à des fins autres que la lutte contre la pandémie et ses effets[53].

Toujours plus présentes dans l'ensemble des dimensions de la vie humaine, les GAFAM[54] ont vu leur puissance croître de façon exponentielle dans les dernières années et leur domination s'est même accrue avec la pandémie de COVID-19 alors que l'économie était en contraction[55]. Cette puissance est aujourd'hui telle que les États les traitent désormais souvent comme des juridictions autonomes[56]. Ces entreprises profitent d'ailleurs largement de la désuétude des cadres législatifs en matière de protection des renseignements personnels et de la vie privée et s'opposent vigoureusement à des modifications législatives qui viendraient limiter leurs capacités à monétiser les données qui appartiennent ultimement aux personnes[57].

---

52 Sebastian KLOVIG SKELTON, « Surveillance capitalism in the age of Covid-19 », *Computer Weekly*, 13 mai 2020, [En ligne]. https://www.computerweekly.com/feature/Surveillance-capitalism-in-the-age-ofCovid-19

53 Par exemple, dans l'État de New York, le gouverneur Andrew Cuomo a nommé l'ancien PDG de Google Eric Schmidt à la tête d'un panel ayant pour tâche de reconfigurer la vie post-COVID en intégrant les technologies numériques dans les différentes facettes de la vie quotidienne. Schmidt et d'autres leaders de l'industrie capitalisent maintenant sur la crise pour stimuler les investissements publics dans cette industrie, accroître l'influence des GAFAM sur le politique et prévenir les régulations en matière de protection de la vie privée. Selon la journaliste et essayiste Naomi KLEIN, la crise du COVID-19 peut donc servir ce qu'elle appelle le capitalisme du désastre, c'est-à-dire que des entreprises privées profitent des « chocs sociétaux » pour faire la promotion de la privatisation et de la dérégulation. Naomi KLEIN, « Screen New Deal », *The Intercept*, 8 mai 2020, [En ligne]. https://theintercept.com/2020/05/08/andrew-cuomo-eric-schmidt-coronavirus-tech-shock-doctrine/

54 L'acronyme réfère à Google (Alphabet Inc.), Apple, Facebook, Amazon et Microsoft.

55 En juillet 2020, Amazon, Apple, Alphabet et Facebook ont annoncé des profits combinés de 28 milliards de dollars états-uniens. Voir Daisuke WAKABAYASHI, Karen WEISE, Jack NICAS et Mike ISAAC, « The Economy Is in Record Decline, but Not for the Tech Giants », *The New York Times*, 30 juillet 2020, [En ligne]. https://www.nytimes.com/2020/07/30/technology/tech-company-earnings-amazon-apple-facebook-google.html; Lawrence DELEVINGNE, « U.S. big tech dominates stock market after monster rally, leaving investors on edge », *Reuters*, 28 août 2020, [En ligne]. https://www.reuters.com/article/us-usa-markets-faangs-analysis-idUSKBN25O0FV; Peter EAVIS et Steve LOHR, « Big Tech's Domination of Business Reaches New Heights », *The New York Times*, 19 avril 2020, [En ligne]. https://www.nytimes.com/2020/08/19/technology/big-tech-business-domination.html

56 M. VEALE, préc., note 51.

57 Par exemple, aux États-Unis, les géants de l'industrie ont fait du lobby auprès du gouvernement fédéral pour l'adoption d'une loi sur la vie privée qui prévaudrait sur le California Consumer Privacy Act. Des groupes représentant Facebook, Google et Twitter ont également profité de la pandémie pour faire valoir un report de l'application de la loi californienne. Voir Cecilia KANG, « Tech Industry Pursues a Federal Privacy Law, on Its Own Terms », *The New York Times*, 26 août 2018, [En ligne]. https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html; David MCCABE,

En vertu des lois encadrant la protection des renseignements personnels au Québec, la collecte de données en ligne exige un consentement plus ou moins explicite entre l'usager et l'entreprise qui offre le contenu, le service ou la plateforme. Or, pour l'usager, il est ardu de savoir quelles données sont collectées, pour quel usage, par qui et quels en sont les effets et les risques[58].

En outre, au-delà de la question de la compréhension des enjeux liés à l'utilisation des produits en ligne et des collectes de données concomitantes, une personne n'a que très peu de contrôle en matière d'accès et d'utilisation de ses données, et ce, compte tenu de la nature de l'écosystème numérique et des rapports de pouvoir dont bénéficient les géants de l'industrie. Comme le notent les chercheuses expertes en médias sociaux Alice E. Marwick et danah boyd :

> […] la vie privée est de plus en plus importante alors que des systèmes algorithmiques gourmands en données sont introduits dans toutes les sphères de la société, s'accaparant des données sur les personnes et leurs pratiques afin de nourrir des systèmes de décision dans des secteurs aussi variés que la justice criminelle, la publicité, le transport et les nouvelles. Le privilège de se retirer (*opt-out*) de ces systèmes axés sur les données est de moins en moins accessible.[59] [Notre traduction.]

Au Québec, en vertu de la *Loi sur la protection des renseignements personnels dans le secteur privé*, pour être valide, le consentement à la collecte, à la communication ou à l'utilisation d'un renseignement personnel doit être manifeste, libre, éclairé et donné à des fins spécifiques et pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé[60]. Notons que les règles de renonciation à exercer un droit garanti par la Charte, tel le droit au respect de sa

---

« How Tech's Lobbyists Are Using the Pandemic to Make Gains », *The New York Times*, 3 avril 2020, [En ligne]. https://www.nytimes.com/2020/04/03/technology/virus-tech-lobbyists-gains.html. En 2019, des documents ont révélé l'étendue d'une opération internationale de lobbying de la part de Facebook à l'endroit de législateurs et de représentants d'autorités régulatrices, notamment au Canada. Voir Carole Cadwalladr et Duncan Campbell, « Revealed : Facebook's global lobbying against data privacy laws », *The Guardian*, 2 mars 2019, [En ligne]. https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment

58 *Le droit à la vie privée à l'ère du numérique*, préc., note 21, par. 18; K. SARIKAKIS et L. WINTER, préc., note 23.

59 Alice E. MARWICK et danah boyd, « Understanding Privacy at the Margins », (2018) 12 *International Journal of Communication* 1158.

60 RLRQ, c. P-39.1, art. 14 (ci-après « Loi sur le privé »).

vie privée[61], présentent des similarités[62]. Dans la mesure où les personnes sont confrontées, plusieurs fois par jour, à la nécessité d'accepter la collecte de leurs données afin d'accéder à des services et des plateformes en ligne dont l'utilisation est de plus en plus incontournable, le consentement ne saurait être libre et éclairé. À cet égard, la professeure de droit Lilian Edwards et le chercheur Michaeal Veale affirment :

> […] le consentement est devenu une devise dévaluée en raison des politiques standards de confidentialité toujours plus longues et des méthodes de « nudging » comme les manipulations de la mise en page de l'écran […] Il est souvent décrit en utilisant des termes comme « inutile » ou « illusoire ».[63]

Une récente analyse du New York Times de 150 politiques de confidentialité de grandes entreprises technologiques conclut qu'elles sont « verbeuses et pleines de jargon juridique – et établissent de façon opaque les justifications des entreprises pour collecter et vendre nos données »[64].

En ce sens, le consentement seul ne constitue pas une protection suffisante et requiert des protections en amont.

Qui plus est, les effets de l'exploitation commerciale des données sur les droits sont systémiques et le contrôle des données ne saurait reposer strictement sur la responsabilité individuelle. Ils commandent donc un encadrement législatif en phase avec l'évolution des nouvelles technologies. De même, l'évaluation des risques associés à des technologies basées sur les données devrait prendre en compte les effets sur les individus, mais aussi sur des groupes marginalisés ou ayant un besoin de protection particulier, notamment les personnes mineures[65].

---

61 Charte, art. 5.

62 Voir *infra* section 2.1.2

63 Lilian EDWARDS et Michael VEALE, « Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For », (2017) 16 *Duke Law & Technology Review* 18, [En ligne]. https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1315&context=dltr

64 Kevin LITMAN-NAVARRO, « We Read 150 Privacy Policies. They Were an Incomprehensible Disaster », *The New York Times*, 12 juin 2019, [En ligne]. https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

65 Kathryn C. MONTGOMERY, Jeff CHESTER et Katharina KOPP, « Health Wearables: Ensuring Fairness, Preventing Discrimination, and Promoting Equity in an Emerging Internet-of-Things Environment », (2018) 8 *Journal of Information Policy* 61, [En ligne]. https://www.jstor.org/stable/pdf/10.5325/jinfopoli.8.2018.0034.pdf

1.3 La vie privée, les inégalités et les discriminations

Le projet de loi vise à modifier les règles de protection des renseignements personnels. Les droits de la personne, dont le droit au respect de sa vie privée[66], sont potentiellement compromis par la collecte, la communication, le traitement et l'utilisation de ces renseignements. Or, les expériences de la vie privée ne sont pas universelles, mais varient plutôt selon les contextes et différents facteurs tels la position sociale, l'âge, le sexe ou la « race ».

C'est également vrai en matière de surveillance. Comme le note le sociologue David Lyon, « Aujourd'hui, la surveillance classe les gens en catégories, en attribuant une valeur ou un risque, de telle façon qu'elle produit des effets réels sur leurs chances dans la vie. Une discrimination profonde s'en suit, faisant ainsi de la surveillance non seulement une question de vie privée, mais de justice sociale »[67].

Cela atteste de l'importance de concevoir le respect de la vie privée comme un droit indivisible, interdépendant et indissociable des autres droits et libertés de la personne, notamment le droit à l'égalité[68]. Comme le soulignent les professeures de droit, d'études médiatiques et de criminologie Jane Bailey, Jacquelyn Burkell et Valerie Steeves :

> Une partie de la solution consiste à briser les silos régulatoires qui traitent la vie privée et les droits de la personne comme des enjeux distincts. Compter sur un modèle de protection des données basé [uniquement] sur le consentement contredit le principe fondamental selon lequel la vie privée et l'égalité sont tous deux des droits de la personne incessibles. […] Afin de lutter contre la discrimination algorithmique, nous devons reconnaître et définir à la fois la vie privée et l'égalité comme des droits de la personne. Et nous devons créer une infrastructure à la fois compétente et attentive à chacune.[69] [Nous soulignons, notre traduction.]

---

66 Charte, art. 5.

67 David LYON, « Introduction », dans David LYON (dir.), *Surveillance as Social Sorting. Privacy, risk and digital discrimination*, Routledge, 2003, p. 2.

68 Charte, art. 10.

69 Jane BAILEY, Jacquelyn BURKELL et Valerie STEEVES, « AI technologies – like police facial recognition – discriminate against people of colour », *The Conversation*, 24 août 2020, [En ligne]. https://theconversation.com/ai-technologies-like-police-facial-recognition-discriminate-against-people-of-colour-143227

Nous reviendrons dans les prochaines parties sur l'inscription de la protection des renseignements personnels dans le cadre structurant du droit au respect à sa vie privée ainsi que sur l'interdépendance de ce droit avec les autres droits et libertés énoncés à la Charte.

Selon la chercheuse Mary Madden, les solutions législatives et technologiques aux violations de la vie privée en ligne doivent prendre en compte les réalités et besoins de protection des communautés marginalisées et en situation de vulnérabilité[70]. Elle montre notamment qu'en dépit du fait qu'elles soient relativement plus nombreuses à exprimer des inquiétudes quant à la collecte et à l'utilisation de leurs données, les personnes avec un faible niveau socioéconomique[71] ou ayant un faible niveau d'éducation sont celles qui ont le moins confiance en leur capacité à protéger leurs informations personnelles en ligne[72].

Les vulnérabilités des personnes pauvres et marginalisées face aux violations de la vie privée s'insèrent dans un contexte global d'inégalités socioéconomiques. Les inquiétudes liées à la vie privée et à la sécurité en ligne chevauchent celles de nature financière[73]. Les répercussions de telles violations peuvent donc être d'autant plus importantes sur la vie quotidienne et le bien-être de ces personnes : « Par exemple, lorsqu'une personne qui vit d'un chèque de paie à l'autre est victime d'une fraude en ligne ou perd sa capacité à utiliser son téléphone intelligent après qu'il ait été piraté, la cascade de répercussions peut être dévastatrice. »[74] [Notre

---

70 Mary MADDEN, « The Devastating Consequences of Being Poor in the Digital Age », *The New York Times*, 25 avril 2019, [En ligne]. https://www.nytimes.com/2019/04/25/opinion/privacy-poverty.html. Voir également Alexandra BAHARY-DIONNE et Karine GENTELET, *Les angles morts des réponses technologiques à la pandémie de COVID-19 : Disjonction entre les inégalités en santé et numériques structurantes de la marginalisation de certaines populations*, Observatoire international sur les impacts sociétaux de l'IA et du numérique, septembre 2020, [En ligne]. https://observatoire-ia.ulaval.ca/rapport-les-angles-morts-des-reponses-technologiques-a-la-pandemie-de-covid-19/

71 En contexte états-unien, certains soulignent que les populations marginalisées, notamment les personnes pauvres, sont exposées à des niveaux plus élevés de surveillance et de collecte de données, notamment dans leurs interactions avec les services sociaux et les services de santé. Voir notamment Virginia EUBANKS, *Automating inequality – How high tech tools profile, police and punish the poor*, New-York, St. Martin's Press, 2017, p. 109.

72 Par exemple, alors que 63 % des personnes avec un diplôme universitaire avaient configuré leur navigateur web pour désactiver les cookies, c'était le cas de seulement 31 % pour celles qui n'ont pas de diplôme secondaire. De façon similaire, 55 % des premiers ont éteint les paramètres de géolocalisation de leurs téléphones, contre 31 % des seconds. Mary MADDEN, *Privacy, Security, and Digital Inequality*, Data & Society Research Institute, 2017, p. 9 et 72. [En ligne]. https://datasociety.net/library/privacy-security-and-digital-inequality/

73 *Id.*, p. 2.

74 *Id.*

traduction.] Qui plus est, le vol d'identité est un phénomène qui générerait des effets disproportionnés sur les personnes à faible revenu, avec des risques accrus pour les personnes en situation de handicap ou allophones[75].

Soulignons par ailleurs que toujours plus de données sont collectées et traitées par des algorithmes complexes dont les calculs et décisions, opaques et incompréhensibles pour celles et ceux y sont soumis, affectent différentes populations de façon inégale. Comme l'a récemment souligné la Commission, le droit à l'égalité[76] peut être compromis par le recours à des systèmes d'intelligence artificielle qui, en dépit de leur apparente neutralité, peuvent avoir des effets discriminatoires sur des catégories de personnes dans une pluralité de secteurs, et ce, notamment en raison de biais inclus dans les données traitées[77].

Le respect des droits des enfants mérite aussi une attention particulière. Par exemple, les violations du droit au respect de la vie privée des enfants peuvent avoir un impact sur leur développement[78]. Tout en ayant un besoin de protection lié à leur situation de vulnérabilité et leur capacité de discernement[79], les enfants et les jeunes accordent une grande importance à la

---

75 Sarah DRANOFF, « Identity Theft : A Low-Income Issue », *Dialogue*, American Bar Association, 15 décembre, [En ligne]. https://www.americanbar.org/groups/legal_services/publications/dialogue/volume/17/winter-2014/identity-theft--a-lowincome-issue/; Alors que les personnes blanches et celles ayant un statut socioéconomique élevé seraient relativement plus nombreuses à rapporter avoir été victimes de vols de données, les répercussions sont susceptibles d'être ressenties plus sévèrement par les personnes racisées ou ayant un statut socioéconomique peu élevé. Pour ces dernières, aux pertes financières et au stress s'ajoutent des risques associés susceptibles de générer des préjudices graves : arrestations erronées, interruptions de versement de prestations de sécurité sociale, harcèlement d'agences de recouvrement, interruptions de service, difficultés d'accès à un logement subventionné, etc. M. MADDEN, préc., note 72, p. 75.

76 Charte, art. 10.

77 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 13, p. 7-8. Voir également Solon BAROCAS et Andrew D. SELBST, « Big Data's Disparate Impact », (2016) 104 *California Law Review* 671.

78 GROUPE DE TRAVAIL DES COMMISSAIRES À LA VIE PRIVÉE ET DES DÉFENSEURS CANADIENS DES ENFANTS ET DES JEUNES SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DES ENFANTS EN LIGNE, *Il devrait y avoir une loi : Les sauts périlleux de la vie privée des enfants au 21e siècle*, 2009, p. 4, Milda MACENAITE et Eleni KOSTA, « Consent for processing children's personal data in the EU: following in US footsteps? », (2017) 26 :2 *Information & Communications Technology Law* 146, p. 146.

79 M. MACENAITE et E. KOSTA, *id.*, p. 147. Par exemple, les enfants et les jeunes ont une difficulté accrue à comprendre les politiques de confidentialité et les mécanismes de consentement : Valerie STEEVES, « Young Canadians in a Wired World, Phase III: Trends and Recommendations », 2015, p. 18 [En ligne]. https://mediasmarts.ca/sites/mediasmarts/files/publication-report/full/ycwwiii_trends_recommendations_fullreport.pdf, GROUPE DE TRAVAIL DES COMMISSAIRES À LA VIE PRIVÉE ET DES DÉFENSEURS CANADIENS DES ENFANTS ET DES JEUNES SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DES ENFANTS EN LIGNE, *id.*, p. 5.

protection de leurs renseignements personnels et de leur vie privée[80]. En même temps, des études démontrent que la présence en ligne, notamment sur les réseaux sociaux, n'est pas considérée comme optionnelle par les jeunes, mais plutôt comme un aspect essentiel de toutes les facettes de leur vie[81]. Cela est tout particulièrement vrai concernant l'accès à des ressources en ligne qui peuvent promouvoir le développement[82] et les droits de certains enfants et jeunes en situation de vulnérabilité, par exemple les enfants et les jeunes LGBTQIA2[83] ou ceux en situation de violence familiale[84]. Finalement, il faut mentionner que certains parents partagent une quantité non négligeable de renseignements personnels de leurs enfants : les photos d'anniversaires permettent de connaître l'âge et la date de naissance de l'enfant, les photos devant l'école permettent de connaître son école et potentiellement son lieu de résidence, les photos de bras dans le plâtre permettent de connaître des informations de santé, etc[85].

Il importe également de considérer la dimension genrée du droit au respect de sa vie privée. Comme le note le Rapporteur spécial des Nations Unies sur le droit à la vie privée, les inégalités fondées sur le genre[86], en interaction avec d'autres motifs de discrimination, affectent

---

80 L'étude « Young Canadians in a Wired World » a révélé qu'ils désirent maintenir un grand contrôle sur qui exactement a accès aux informations qu'ils partagent. Dans cette même étude, 95 % des participants s'opposaient à l'accès à leurs informations pour des fins de prospection commerciale. Presque tous s'opposaient à l'utilisation de leurs données de géolocalisation. V. STEEVES, *id*., p. 11-12.

81 Jane BAILEY et Valerie STEEVES, *Online Reputation, Privacy and Young People: Lessons from Canadian Research*, 2016, p. 2-3 [En ligne]. http://www.equalityproject.ca/wp-content/uploads/2016/04/01-Bailey-Steeves-Online-Reputation-Submission-FINAL-April-27-2016.pdf. Selon un rapport de EU Kids Online, près de 50% des enfants âgées de 11 à 16 ans trouvent plus facile d'être soi-même en ligne que face à face : EU KIDS ONLINE NETWORK, *EU Kids Online: Findings, methods, recommendations*, 2014, p. 31 [En ligne] : <http://eprints.lse.ac.uk/60512/1/EU%20Kids%20onlinie%20III%20.pdf> (consulté le 16 septembre 2020).

82 Valerie STEEVES et Priscilla REGAN , « Young people online and the social value of privacy», (2014) 12-4 *Journal of Information, Communication and Ethics in Society* 298 p. 303.

83 Diane KEATS CITRON, *Hate Crimes in Cyberspace*, Cambridge, Harvard University Press, 2014, p. 60-61.

84 M. MACENAITE et E. KOSTA préc., note 78, p. 163, UNICEF, *Discussion Paper Series: Children's Rights and Business in a Digital World: Privacy, Protection of Personal Information and Reputation Rights,* 2017 [En ligne]. https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf , p. 9. Voir à cet effet : *Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*, (UE) 2016/679, 38e considérant du Préambule (ci-après « RGPD »).

85 Voir à ce sujet : OPTION CONSOMMATEURS, *Être parent à l'ère du numérique, Le partage de renseignements personnels sur les réseaux sociaux et ses conséquences sur le droit à la vie privée et à l'image des enfants*, 2019, [En ligne]. https://option-consommateurs.org/wp-content/uploads/2019/09/parentalite-numerique-oc.pdf

86 Le genre inclut ici la cisnormativité, le sexe biologique, l'orientation sexuelle, l'expression et l'identité de genre, les caractéristiques sexuelles et les normes sociales associées. HUMAN RIGHTS COUNCIL, *Report of the*

la façon dont les personnes expérimentent les technologies numériques et la vie privée[87]. Il rappelle que « la protection de la vie privée offre une protection contre la violence discriminatoire fondée sur le genre et les autres préjudices qui affectent de manière disproportionnée les femmes, les personnes intersexes et les personnes non conformes au genre ».[88] [Notre traduction.]

Par ailleurs, dans les relations intimes, peu importe le genre, les personnes qui abusent ont de plus en plus recours à des outils technologiques relativement faciles d'accès pour surveiller et contrôler leurs victimes sur la base de leurs données de géolocalisation, communications numériques et autres[89]. Les personnes appartenant à une minorité sexuelle seraient particulièrement plus à risque d'être victimes de tels abus[90].

Special Rapporteur on the right to privacy, A/HRC/43/52, 12 février 2020, par. 20 (d) i), [En ligne]. https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session43/Documents/A_HRC_43_52_AdvanceUneditedVersion.docx

87 HUMAN RIGHTS COUNCIL, *Right to privacy, Report of the Special Rapporteur on the right to privacy*, A/HRC/40/63, 27 février 2019, par. 57, [En ligne]. https://rm.coe.int/40th-hrc-session-report-of-the-special-rapporteur-on-the-right-to-priv/1680933f08

88 HUMAN RIGHTS COUNCIL, *Report of the Special Rapporteur on the right to privacy*, A/HRC/43/52, 12 février 2020, par. 19 (e), [En ligne]. https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session43/Documents/A_HRC_43_52_AdvanceUneditedVersion.docx

89 Voir Karen LEVY et Bruce SCHNEIER, « Privacy threats in intimate relationships », (2020) 6:1 *Journal of Cybersecurity*, [En ligne]. https://academic.oup.com/cybersecurity/article/6/1/tyaa006/5849222?searchresult=1 ; Diane FREED, Jackeline PALMER, Diana MINCHALA, Karen LEVY, Thomas RISTENPART et Nicola DELL, « 'A Stalker's Paradise': How Intimate Partner Abusers Exploit Technology », Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI) 2018, [En ligne]. http://nixdell.com/papers/stalkers-paradise-intimate.pdf

90 Michelle YBARRA, Myeshia PRICE-FEENEY, Amanda LENHART et Kathryn ZICKUHR, *Intimate Partner Digital Abuse*, Data&Society Research Institute, Center for Innovative Public Health Research, 18 janvier 2017, [En ligne]. https://datasociety.net/wp-content/uploads/2017/01/Intimate_Partner_Digital_Abuse_2017.pdf; Au Canada, ces personnes sont largement plus susceptibles de déclarer être victimes de comportements inappropriés en ligne comme hors ligne. Voir Brianna JAFFRAY, « Les expériences de victimisation avec violence et de comportements sexuels non désirés vécues par les personnes gaies, lesbiennes, bisexuelles et d'une autre minorité sexuelle, et les personnes transgenres au Canada, 2018 », 9 septembre 2020, No 85-002-X au catalogue de Statistique Canada, [En ligne]. https://www150.statcan.gc.ca/n1/fr/pub/85-002-x/2020001/article/00009-fra.pdf?st=6rPSL2mC

1.4 La surveillance policière

La Commission a déjà exprimé ses préoccupations quant aux effets de la surveillance vidéo généralisée par l'État sur l'exercice de plusieurs droits protégés par la Charte[91].

À cet égard, avec le développement des nouvelles technologies, la collecte et le traitement de données par les agences gouvernementales et les services policiers en partenariat avec des entreprises privées du secteur des technologies sont la source d'inquiétudes grandissante quant à la protection des droits et libertés[92]. La surveillance policière algorithmique repose sur l'agrégation et l'analyse automatisée de données massives de diverses sources et natures : informations personnelles, données de communications, de géolocalisation, images, contenus des médias sociaux et données policières[93]. Aussi bien le volume que la diversité des types de renseignements personnels collectés par la police sont inédits.

Dans son mémoire sur les orientations gouvernementales intitulé « Plus de transparence pour une meilleure gouvernance », la Commission s'inquiétait de ce que « [l] es moyens technologiques de l'ère numérique ont renforcé la capacité des organismes publics de surveiller, intercepter et collecter les données »[94]. Elle ajoutait :

> Les activités de police, à l'instar de toutes les activités de surveillance de l'État, doivent être examinées afin de vérifier si elles entraînent une atteinte au droit au respect de la vie privée. Si tel est le cas, une évaluation de l'activité au regard de l'article 9.1 de la Charte doit être effectuée. En outre, la notification de l'existence d'un régime de surveillance

---

91 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Mémoire à la Commission d'accès l'information. La surveillance vidéo dans les lieux publics par les organismes publics : son incidence sur les droits protégés par la Charte*, (Cat. 2.110.1), 2003, [En ligne]. https://www.cdpdj.qc.ca/storage/app/media/publications/surveillance_lieux_publics.pdf

92 Le Haut-Commissariat des Nations Unies aux droits de l'homme a d'ailleurs souligné l'inquiétante normalisation de la surveillance numérique de masse par les États : *Le droit à la vie privée à l'ère du numérique*, préc., note 21, par. 3.

93 K. ROBERTSON, C. KHOO et Y. SONG, préc., note 22, p. 75.

94 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Mémoire à la Commission des institutions de l'Assemblée nationale sur le document d'orientation intitulé « Plus de transparence, pour une meilleure gouvernance : Orientations gouvernementales pour un gouvernement plus transparent, dans le respect du droit à la vie privée et la protection des renseignements personnels »,* (Cat. 2.412.42.6), 2015, p. 19 [renvoi omis], [En ligne]. https://cdpdj.qc.ca/storage/app/media/publications/memoire_transparence-gouvernance.pdf .

> générale ou d'un régime de surveillance spécifique devient cruciale à l'exercice d'un recours utile en matière de droits de la personne.[95]

Notons que les enjeux liés à l'utilisation des nouvelles technologies sont abordés dans le livre vert *Réalité policière au Québec : modernité, confiance et efficience*[96] qui fait actuellement l'objet d'une consultation publique[97]. Le ministère de la Sécurité publique y énonce que le travail des policiers est facilité par le développement des nouvelles technologies de l'information, notamment en ce qui concerne l'intelligence artificielle et les médias sociaux[98]. Citant en exemple l'utilisation d'outils comme les radars photo[99] et les caméras corporelles, on y souligne que « les questions relatives à la confidentialité des données [et] au respect des droits fondamentaux […] sont toutefois des enjeux importants dont il faut tenir compte »[100]. En effet, de nombreuses études documentent les risques en matière de protection des droits et libertés de la personne encourus par le recours aux nouvelles technologies dans les opérations des forces de l'ordre.

Commentant l'utilisation des données biométriques par les forces de police à travers le recours aux logiciels de reconnaissance faciale, la professeure de droit Céline Castets-Renard et ses collègues notent que « l'insuffisance du cadre légal est flagrante aujourd'hui », et ce, en raison du fait qu'« aucune disposition législative spécifique n'est prévue pour protéger davantage ce type de données à risques »[101]. Pour sa part, la CAI considère les renseignements biométriques

---

95 *Id.*, p. 20.

96 MINISTÈRE DE LA SÉCURITÉ PUBLIQUE, *Réalité policière au Québec. Modernité, confiance et efficience*, Québec, Gouvernement du Québec, 2019, p. 24.

97 MINISTÈRE DE LA SÉCURITÉ PUBLIQUE, « Réalité policière au Québec - Le comité consultatif présente son plan de travail révisé », communiqué, 8 juin 2020.

98 MINISTÈRE DE LA SÉCURITÉ PUBLIQUE, préc., note 96, p. 24.

99 Voir COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Mémoire à la Commission des transports et de l'environnement de l'Assemblée nationale. Projet de loi nº 17, Loi modifiant le Code de la sécurité routière et le Code de procédure pénale concernant le cinémomètre photographique*, (Cat. 2.412.35.3), 2001, [En ligne]. https://www.cdpdj.qc.ca/storage/app/media/publications/Cinemometre.pdf; COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Mémoire à la Commission des transports et de l'environnement de l'Assemblée nationale. Projet de loi nº 57, Loi modifiant l'encadrement de l'utilisation cinémomètres photographiques et d'autres dispositions législatives*, (Cat. 2.412.35.4), 2012, [En ligne]. https://www.cdpdj.qc.ca/storage/app/media/publications/memoire_PL_57_cinemometre_photo.pdf

100 MINISTÈRE DE LA SÉCURITÉ PUBLIQUE, préc., note 96, p. 24.

101 Céline CASTETS-RENARD, Émilie GUIRAUD et Jacinthe AVRIL-GAGNON, *Cadre juridique applicable à l'utilisation de la reconnaissance faciale par les forces de police dans l'espace public au Québec et au Canada. Éléments de comparaison avec les États-Unis et l'Europe*, Observatoire international sur les impacts

comme des données personnelles, mais reconnaît que le cadre légal qui s'y applique est méconnu[102]. Or comme l'indiquent Castet-Renard et collègues :

> [I] l existe déjà au Québec une législation qui a vocation à encadrer les technologies fondées sur la biométrie. Il convient cependant aujourd'hui de vérifier si cette législation encadre toujours adéquatement le déploiement des technologies fondées sur la biométrie, en particulier dans le cadre de son utilisation par les forces de police dans l'espace public.[103]

Selon les auteures d'une étude du Citizen Lab de l'Université de Toronto sur la surveillance policière algorithmique au Canada, l'absence d'encadrement légal spécifique de la reconnaissance faciale pose certains défis au respect du droit à la vie privée comme l'érosion de l'anonymat dans la vie quotidienne; la collecte, la rétention et le traitement des renseignements personnels sans le consentement des titulaires; un accroissement des risques d'arrestations erronées pour les femmes et les personnes racisées, notamment celles à la peau foncée; ainsi qu'un déficit de transparence, de contrôle et de balises quant à l'usage des données dans les relations étroites entre le secteur privé et les services de police[104]. Notons au passage que la question de la transparence en la matière a été soulevée dans le bilan de la mise en œuvre des recommandations du rapport de consultation de la Commission des droits de la personne et des droits de la jeunesse sur le profilage racial et ses conséquences[105].

La collaboration entre la police et l'entreprise privée en matière de surveillance a récemment été au cœur de plusieurs controverses, particulièrement en regard de l'utilisation de la reconnaissance faciale.

---

sociétaux de l'IA et du numérique, Chaire de recherche I.A. responsable à l'échelle mondiale, 2020, p. 54. [En ligne]. https://observatoire-ia.ulaval.ca/rapport-reconnaissance-faciale/

102 COMMISSION D'ACCÈS À L'INFORMATION, *Biométrie : Principes à respecter et obligations légales des organisations, Guide d'accompagnement pour les organismes publiques et les entreprises*, 2020, [En ligne]. https://observatoire-ia.ulaval.ca/rapport-reconnaissance-faciale/

103 C. CASTET-RENARD, É. GUIRAUD et J. AVRIL-GAGNON, préc., note 101, p. 45.

104 K. ROBERTSON, C. KHOO et Y. SONG, préc., note 22, p. 90-93.

105 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Bilan de la mise en œuvre des recommandations du Rapport de la consultation de la Commission des droits de la personne et des droits de la jeunesse sur le profilage racial et ses conséquences*, Me Evelyne PEDNEAULT et Amina TRIKI-YAMANI, 2020, p. 88, [En ligne]. https://www.cdpdj.qc.ca/storage/app/media/publications/bilan-profilage-racial.pdf

La Haute-Commissaire des Nations Unies aux droits de l'homme exprimait récemment des inquiétudes quant à la protection des droits fondamentaux en lien avec la conception et l'utilisation des nouvelles technologies, dont la reconnaissance faciale. Elle a notamment appelé à la tenue d'un moratoire sur l'utilisation de la technologie dans le cadre de manifestations pacifiques, et ce jusqu'à ce que les États satisfassent les conditions suivantes : « une surveillance efficace et indépendante de son utilisation, des lois strictes sur la protection de la vie privée et des données, et une transparence totale quant à l'utilisation des enregistrements d'images et de la technologie de reconnaissance faciale dans le contexte des rassemblements »[106].

Au Canada, il a été révélé que la GRC et 34 services policiers ont utilisé le logiciel développé par Clearview AI qui opère à partir de données massives collectées sur les médias sociaux sans le contentement des détenteurs des renseignements[107]. Dans ce contexte, le Service de police de la Ville de Montréal (SPVM) a d'abord refusé de communiquer à la Commission de la sécurité publique de la Ville de Montréal l'information à savoir s'il possédait et utilisait ce logiciel ou tout autre logiciel de reconnaissance faciale[108]. Il a ensuite rapporté que ses agents n'utilisaient pas le logiciel de Clearview[109], tout en notant que « [l]'organisation n'exclut toutefois pas, dans des situations particulières et exceptionnelles, de recourir aux services d'une tierce partie possédant ce type de technologie pour faire avancer une enquête d'envergure, en

---

106 HAUT-COMMISSARIAT DES NATIONS UNIES AUX DROITS DE L'HOMME, « Les nouvelles technologies doivent favoriser et non entraver le droit de manifester pacifiquement, annonce Michelle Bachelet aux États », 25 juin 2020, [En ligne]. https://www.ohchr.org/fr/NewsEvents/Pages/DisplayNews.aspx?NewsID=25996&LangID=f

107 Kashmir HILL, « The Secretive Company That Might End Privacy as We Know It », *The New York Times*, 18 janvier 2020, [En ligne]. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; Nicholas DE ROSA, « La GRC et 44 services policiers canadiens ont utilisé l'application de Clearview AI », *Radio-Canada*, 28 février 2020, [En ligne]. https://ici.radio-canada.ca/nouvelle/1641195/clearview-ai-canada-police-grc-entreprise-via-rail-liste-client-vol-donees-intelligence-artificielle-reconnaissance-faciale-logiciel-application-controverse

108 Tristan PÉLOQUIN, « Reconnaissance faciale : le SPVM refuse de dire s'il utilise un logiciel controversé », 18 février 2020, [En ligne]. https://www.lapresse.ca/actualites/grand-montreal/2020-02-18/reconnaissance-faciale-le-spvm-refuse-de-dire-s-il-utilise-un-logiciel-controverse

109 L'entreprise a finalement retiré son offre de services au Canada en juillet 2020, et ce, après l'ouverture d'une enquête conjointe menée par le Commissariat à la protection de la vie privée du Canada, la CAI et leurs homologues albertains et britanno-colombiens. LA PRESSE CANADIENNE, « Clearview abandonne son service de reconnaissance faciale au Canada « , *Radio-Canada*, 6 juillet 2020, [En ligne]. https://ici.radio-canada.ca/nouvelle/1717708/intelligence-artificielle-clearview-ai-protection-vie-privee-canada

s'assurant toujours de mener ses opérations et ses enquêtes dans le respect de toutes les lois en vigueur[110] ».

On apprenait récemment que la Sûreté du Québec (SQ) a conclu un contrat avec la société française Idemia pour des « solutions clé en main » de reconnaissance faciale et d'empreintes digitales[111]. Selon la SQ, la technologie de reconnaissance faciale sera utilisée « dans le cadre d'enquêtes criminelles pour comparer des images de caméras de surveillance à une base de données comptant des dizaines de milliers de photos signalétiques (*mugshots*) de personnes ayant un dossier criminel ou ayant fait l'objet d'enquêtes[112] ». Notons que, dans une étude fédérale états-unienne, le système d'Idemia était parmi ceux qui présentaient les plus faibles marges d'erreur pour les visages de femmes et de minorités racisées. Toutefois, le taux d'identifications erronées demeurait dix fois plus élevé pour les femmes noires que pour les femmes blanches[113]. Plusieurs études documentent en effet les biais genrés et raciaux et les effets discriminatoires des systèmes de reconnaissance faciale offerts sur le marché[114] Notons que l'usage de la technologie a fait l'objet de critiques pour cette raison dans la foulée des

---

110 Cité dans Isabelle DUCAS, « Pas de reconnaissance faciale par les policiers sans l'accord des élus », *La Presse*, 22 septembre 2020, [En ligne]. https://www.lapresse.ca/actualites/2020-09-22/montreal/pas-de-reconnaissance-faciale-par-les-policiers-sans-l-accord-des-elus.php

111 *Id.*

112 Tristan PÉLOQUIN, « Reconnaissance faciale : la SQ pourrait acquérir une technologie controversée », *La Presse*, 22 juin 2020, [En ligne]. https://www.lapresse.ca/actualites/justice-et-faits-divers/2020-06-22/reconnaissance-faciale-la-sq-pourrait-acquerir-une-technologie-controversee

113 Voir Tom SIMONITE, « The Best Algotihms Struggle to Recognize Black Faces Equally », *The Wired*, 22 juillet 2019, [En ligne]. https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/

114 Voir notamment, Joy BUOLAMWINI et Timnit GEBRU, « Gender Shades : Intersectional Accuracy Disparities in Commercial Gender Classification » (2018) 81 *Proceedings of Machine Learning Research* 1, [En ligne]. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; Drew HARWELL, « Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use », *The Washington Post*, 19 décembre 2019, [En ligne]. https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facialrecognition-systems-casts-doubt-their-expanding-use/ ; Joy BUOLAMWINI, « We Must Fight Face Surveillance to Protect Black Lives », *Medium*, 3 juin 2020, [En ligne]. https://onezero.medium.com/we-must-fight-face-surveillance-to-protect-black-lives-5ffcd0b4c28a. Des experts en intelligence articifielle ont également signés lettres ouvertes contre l'utilisation de la reconnaissance faciale par la police. Voir « Open Letter to Amazon against Police and Government use of Rekognition », [En ligne]. https ://www.icrac.net/open-letter-to-amazon-against-police-and-government-use-of-rekognition/; On Recent Research Auditing Commercial Facial Analysis Technology, 26 mars 2019, [En ligne]. https://medium.com/@bu64dcjrytwitb8/on-recent-research-auditing-commercial-facial-analysis-technology-19148bda1832. En juin dernier, dans la foulée des protestations contre le racisme au sein des forces policières faisant suite à la mort de l'Afro-Américain George Floyd, IBM, Amazon et Microsoft ont annoncé qu'ils arrêtaient ou mettaient sur pause la vente de logiciels de reconnaissance faciale aux forces de l'ordre, arguant en faveur de l'adoption, aux États-Unis, d'une législation fédérale afin de protéger les droits de la personne.

protestations contre le racisme au sein des forces policières à la suite de la mort de l'Afro-Américain George Floyd[115].

À ce sujet, dans son rapport *Racisme et discrimination systémiques dans les compétences de la Ville de Montréal* de juin 2020, l'Office de consultation publique de Montréal émettait la recommandation suivante au sujet de l'utilisation de la reconnaissance faciale par le SPVM :

> La commission recommande que la Ville de Montréal entreprenne les actions suivantes, d'ici l'échéance du présent mandat du directeur du SPVM :
>
> - mener et publier les résultats d'une analyse éthique et criminologique en collaboration avec des équipes de recherche montréalaises avant que le SPVM déploie toute technologie de prévision policière et de reconnaissance faciale à grande échelle;
> - encadrer toute éventuelle utilisation de ces technologies pour qu'elles n'amplifient pas le profilage racial et social.[116]

En septembre 2020, le conseil municipal de la Ville de Montréal a adopté une motion exigeant que le SPVM demande son autorisation avant de faire l'acquisition d'outils de reconnaissance faciale et qu'il dévoile annuellement l'utilisation de technologie de surveillance et des données

---

115 D'ailleurs, IBM, Amazon et Microsoft ont annoncé qu'ils arrêtaient ou mettaient sur pause la vente de logiciels de reconnaissance faciale aux forces de l'ordre, arguant en faveur de l'adoption, aux États-Unis, d'une législation fédérale afin de protéger les droits de la personne. Voir Isobel ASHER HAMILTON, « Outrage over police brutality has finally convinced Amazon, Microsoft, and IBM to rule out selling facial recognition tech to law enforcement. Here's what's going on. », *Business Insider*, 13 juin 2020, [En ligne]. https://www.businessinsider.com/amazon-microsoft-ibm-halt-selling-facial-recognition-to-police-2020-6. Notons que plusieurs chercheurs et personnes ou groupes militant depuis des années en faveur de l'adoption de réglementations sur la question sont sceptiques devant ce nouveau discours d'une entreprise comme Amazon qui fait du lobby afin d'éviter la régulation du secteur. Certains considèrent ces annonces comme étant opportunistes dans la mesure où d'autres outils technologiques qui portent atteinte aux droits de la personne sont développés et vendus aux forces de l'ordre. D'autres s'inquiètent du fait que de telles entreprises influencent l'adoption d'une législation fédérale afin d'éviter de devoir composer avec un ensemble de législations régionales qui peuvent être plus contraignantes. Voir notamment Kate KAYE, « IBM, Microsoft, and Amazon's face recognition bans don't go far enough » *Fast Company*, 13 juin 2020, [En ligne]. https://www.fastcompany.com/90516450/ibm-microsoft-and-amazons-face-recognition-bans-dont-go-far-enough?partner=rss&utm_source=rss&utm_medium=feed&utm_campaign=rss+fastcompany&utm_content=rss?cid=search; Karen HAO, « The two-year fight to stop Amazon from selling face recognition to the police », *MIT Technology Review*, 12 juin 2020, [En ligne]. https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/

116 OFFICE DE CONSULTATION PUBLIQUE DE MONTRÉAL, *Racisme et discrimination systémiques dans les compétences de la Ville de Montréal*, Rapport de consultation publique, 3 juin 2020, p. 165, [En ligne]. https://ocpm.qc.ca/sites/ocpm.qc.ca/files/pdf/P99/rapport-reds.pdf

liées à la Commission de la sécurité publique[117]. Soulignons que la motion fait notamment mention d'inquiétudes quant à la protection des renseignements personnels, au respect de sa vie privée et à la surveillance discriminatoire à des fins d'intimidation et d'oppression de groupes protégés par la Charte[118]. Cette volonté d'encadrer l'utilisation de la technologie fait notamment écho aux initiatives observées dans des juridictions à l'international.

En Europe, s'il n'existe pas encore de législation spécifique portant sur la reconnaissance faciale[119], la directive 2016/680/UE et ses déclinaisons nationales encadrent le traitement de données biométriques par la police et la justice et cette directive est applicable à l'utilisation de la reconnaissance faciale[120]. Selon Castets-Renard et ses collègues, à ce jour, seuls les tribunaux du Royaume-Uni ont tranché à propos du recours à la reconnaissance faciale par des services policiers[121]. Dans l'affaire *R (Bridges)* c. *Chief Constable of South Wales*, la Cour d'appel d'Angleterre et du Pays de Galles a jugé que l'utilisation indiscriminée et disproportionnée de la reconnaissance faciale par la Police de la Galles du Sud violait l'article 8 de la *Convention européenne des droits de l'homme*[122] garantissant le droit à la vie privée et que l'évaluation d'impact sur la protection des données (DPIA) a échoué à évaluer adéquatement les risques pour les droits et libertés des détenteurs de données[123]. La Cour a également jugé que le service de police a manqué à ses obligations en matière d'égalité en ne

---

117 I. DUCAS, préc., note 110. Cela fait écho aux ordonnances promulguées par des villes aux États-Unis, notamment en Californie, au Massachusetts et à New York. Voir. C. CASTETS-RENARD, É. GUIRAUD et J. AVRIL-GAGNON, préc., note 101, p. 73-77.

118 VILLE DE MONTRÉAL, *Assemblée ordinaire du conseil municipal. Version 2*, 21 septembre 2020, p. 131. [En ligne]. https://ville.montreal.qc.ca/documents/Adi_Public/CM/CM_ODJ_LPP_ORDI_2020-09-21_13h00_FR.pdf

119 Voir Caroline LEQUESNE ROTH (dir.), *La reconnaissance faciale dans l'espace public : Une cartographie juridique européenne*, Rapport de la Fablex DL4T, avril 2020, [En ligne]. https://dl4t.org/wp-content/uploads/2020/05/RF-V1-Fablex-2020.pdf

120 C. CASTETS-RENARD, É. GUIRAUD et J. AVRIL-GAGNON, préc., note 101, p. 64.

121 *R (Bridges)* v. *CC South Wales*, [2020] EWCA Civ 1058, Case No : C1/2019/2670, in the Court of Appeal (civil division) on appeal from the High Court of Justice Queen's Bench Division (administrative court), [En ligne]. https://www.judiciary.uk/judgments/r-bridges-v-cc-south-wales. Le recours à la reconnaissance faciale a aussi été jugé et invalidé en France en contexte scolaire. C. CASTETS-RENARD, É. GUIRAUD et J. AVRIL-GAGNON, *id.*, p. 66.

122 *Convention de sauvegarde des droits de l'homme et des libertés fondamentales*, 4 novembre 1950, 213 R.T.N.U. 221 (entrée en vigueur le 3 septembre 1953).

123 *R (Bridges)* v *CC South Wales*, préc., note 121, par. 210, 1), 2).

cherchant pas à s'assurer que la technologie utilisée n'entraîne pas de discrimination indirecte basée sur la « race » et le genre[124].

De nombreuses juridictions municipales et étatiques états-uniennes ont adopté des mesures législatives sur la question[125]. Si, au niveau des juridictions municipales, la reconnaissance faciale n'a pas été interdite, mais plutôt encadrée, des États ont imposé des moratoires ou interdit la reconnaissance faciale dans les écoles ou en combinaison avec des drones ou des caméras corporelles[126].

À l'international comme au Québec, les demandes se font donc de plus en plus nombreuses pour l'encadrement législatif de la collecte et de l'utilisation de renseignements personnels par l'utilisation de la technologie de reconnaissance faciale. D'autres nouvelles technologies sont adoptées pour collecter et utiliser des renseignements personnels dans le cadre d'opérations policières.

La littérature documente notamment bien le fait que des pouvoirs étatiques et des forces policières ont recours aux données disponibles sur les médias sociaux pour surveiller et contrôler les actions des citoyens[127]. La Commission s'est déjà prononcée sur la question :

> Les moyens technologiques de l'ère numérique ont renforcé la capacité des organismes publics de surveiller, intercepter et collecter les données. Les orientations gouvernementales tiennent comptent de ces préoccupations quand elles abordent des questions « telles que la publicité comportementale en ligne, la géolocalisation et la reconnaissance faciale », le traitement massif des données, « les besoins grandissants en matière d'échanges de renseignements personnels entre les organismes publics pour, notamment, contrer la fraude » et « les enjeux liés à la cybersurveillance, dans l'objectif de sécurité nationale et internationale »[128] [Renvois omis].

---

124 *Id.*, par. 200 et 201.

125 C. CASTETS-RENARD, É. GUIRAUD et J. AVRIL-GAGNON, préc., note 101, p. 73, 80.

126 *Id.*, p. 77-80.

127 D. TROTTIER et C. FUCHS, préc., note 23, p. 3; Stephen OWEN, « Monitoring social media and protest movements: ensuring political order through surveillance and surveillance discourse » (2017) 23:6 *Social Identities* 688; Elizabeth E. JOH, « The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing », (2015) 10:1 *Harvard Law & Policy Review* 15, [En ligne]. https://harvardlpr.com/wp-content/uploads/sites/20/2016/02/10.1_3_Joh.pdf; F. H. CATE, J. X. DEMPSEY et I. S. RUBINSTEIN, préc., note 21, p. 195.

128 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 21, p. 19.

Elle ajoutait :

> Ici comme ailleurs, les règles encadrant la protection des renseignements personnels sont souvent écartées au titre de l'exercice de la mission de surveillance de l'État. Rappelons cependant que la Charte lie l'État et que l'ensemble de l'action gouvernementale doit donc être conforme aux droits et libertés énoncés à la Charte[129].

Au Canada, la police collecterait et traiterait donc des données qu'elle juge ne pas être protégées par le droit à la vie privée: « En fait, les assertions controversées des forces policières voulant que ces informations soient disponibles gratuitement et qu'elles soient libres de les utiliser aux fins du maintien de l'ordre tirent leur source du fait qu'il n'existe pas de loi qui permette ou interdise spécifiquement cette collecte. »[130] [Notre traduction.] Des auteures notent que la surveillance algorithmique pourrait porter atteinte au droit à la vie privée et violer l'article 8 de la Charte canadienne lorsque ces technologies sont utilisées sans contrôle judiciaire ou sans considération pour les principes de nécessité et de proportionnalité[131]. Nous reviendrons à la section 3 sur les atteintes liées notamment à l'article 24.1 de la Charte québécoise, similaire à l'article 8 de la Charte canadienne.

Les « citoyens transparents » accroissent leur visibilité en produisant, sur les plateformes numériques une quantité inédite d'informations susceptibles d'être utilisées pour le travail policier, ce qui ouvre la voie à des pratiques de profilage et de « preemptive policing »[132]. Les technologies d'analyse automatisées des métadonnées développées à des fins de marketing par le secteur commercial sont aujourd'hui partie intégrante de régimes de surveillance étatiques, notamment pour le contrôle des manifestations, ce qui soulève des questions quant à la protection des droits et libertés démocratiques[133], notamment des libertés fondamentales

---

129 *Id.*, p. 21-22.

130 K. ROBERTSON, C. KHOO et Y. SONG, préc., note 22, p. 75.

131 *Id.*

132 Daniel TROTTIER, « Policing Social Media », (2012) 49-4 *Revue Canadienne de sociologie* 411.

133 Lina DENCIK, Arne HINTZ et Zoe CAREY, « Prediction, pre-emption and limits to dissent: Social media and big data uses for policing protests in the United Kingdom », (2018) 20-4 *new media & society.* 1433; Desmond Upton PATTON, Douglas-Wade BRUNTON, Andrea DIXON, Reuben Jonathan MILLER, Patrick LEONARD et Rose HACKMAN, « Stop and Frisk Online: Theorizing Everyday Racism in Digital Policing in the Use of Social Media for Identification of Criminal Conduct and Associations », (2017) 3-3 *Soc. Media Soc.* 205630511773334, DOI : 10.1177/2056305117733344., p. 3; K. ROBERTSON, C. KHOO et Y. SONG, préc., note 22, p. 97-100.

telles que la liberté d'expression et de réunion pacifique[134], ainsi que du droit à l'exercice de ces libertés en pleine égalité, sans distinction fondée sur un motif de discrimination énoncé à la Charte[135]. La surveillance et les atteintes à la vie privée qui y sont liées ont des impacts variés sur différentes populations visées par ces motifs. La Commission s'inquiète notamment des profilages racial[136], social[137] et politique[138] que subissent certains groupes. Plusieurs enquêtes et études montrent d'ailleurs que des minorités racisées sont l'objet de pratiques de surveillance policière ciblées sur les réseaux sociaux[139].

Dans la mesure où les personnes se sauraient observées, le développement de nouvelles technologies de surveillance est aussi susceptible de contribuer à la modification des comportements en fonction de la conduite attendue[140] et d'ainsi porter atteinte à l'exercice de

134 Charte, art. 3.

135 Charte, art. 10.

136 Voir, notamment, COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Profilage racial et discrimination systémique des jeunes racisés*, Rapport de la consultation sur le profilage racial et ses conséquences, Paul Eid, Johanne Magloire et Me Michèle Turenne, 2011, [En ligne]. https://www.cdpdj.qc.ca/storage/app/media/publications/Profilage_rapport_FR.pdf; COMMISSION DE DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 105.

137 Voir entre autres COMMISSION DE DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *La judiciarisation des personnes itnérantes à Montréal : Un profilage social*, Me Christine Campbell et Paul Eid, (Cat. 2.120-8.61), 2009, [En ligne]. https://cdpdj.qc.ca/storage/app/media/publications/itinerance_avis.pdf ; COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Mémoire à la Commission sur le développement social et la diversité montréalaise à la Commission sur la sécurité publique de la Ville de Montréal dans le consultation sur la lutte au profilage racial et au proficial social*, (Cat. 2.120-1.33), 2017, [En ligne]. https://cdpdj.qc.ca/storage/app/media/publications/Bilan_Mtl_profilages_racial_social.pdf

138 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSSE, « Profilage politique : La Commission des droits de la personne et des droits de la jeunesse soumet une première cause au Tribunal des droits de la personne », Communiqué de presse, 3 juillet 2015, [En ;igne]. https://cdpdj.qc.ca/fr/actualites/profilage-politique-la-commis-2

139 Voir notamment Stephen DAVIS, « Police monitored Black Lives Matter Toronto protesters in 2016, documents show », *CBC*, 3 mai 2018, [En ligne]. https://www.cbc.ca/news/canada/toronto/police-monitored-black-lives-matter-toronto-protesters-in-2016-documents-show-1.4645628; Sam BIDDLE, « Police surveilled George Floyd protests with help from Twitter-affiliated startup Dataminr », *The Intercept*, 9 juillet 2020, [En ligne]. https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests/; D. PATTON et al., préc., note 133; THE CITY UNIVERSITY OF NEW YORK SCHOOL OF LAW, « Raza v. City of New York », [En ligne]. https://www.law.cuny.edu/academics/clinics/immigration/clear/raza/; Mark LATONERO et Paula KIFT, « On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control » (2018) (janvier-mars) *Social Media + Society* 1, [En ligne]. https://journals.sagepub.com/doi/pdf/10.1177/2056305118764432

140 Ivan MANOKHA, « Surveillance, Panopticism, and Self-Discipline in the Digital Age », (2018) 16 :2 *Surveillance & Society*, p. 219, [En ligne]. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/8346/7674; Jon PENNEY, « Internet Surveillance, Regulation, and Chilling Effects Online » (2017) 6:2 *Internet Policy Review*, [En ligne]. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959611

différents droits et libertés protégés par la Charte, notamment le droit à la liberté de sa personne[141], la liberté d'expression et d'association[142] et le droit à l'information[143].

1.5 La surveillance et le travail

Les dispositifs et technologies de surveillance sont rarement neutres dans la mesure où ils ont tendance à être d'abord imposés à des populations qui disposent de moins de pouvoir pour s'y opposer et donc à renforcer des situations d'inégalités[144].

Dans la sphère du travail, les travailleurs précaires ou à faible revenu sont particulièrement exposés à des formes de surveillance et à des risques de violations de la privée, et ce, en raison des asymétries de pouvoir inhérentes à la relation entre employeur et employé[145]. Pensons par exemple aux effets discriminatoires des vérifications de crédit sur lesquels la Commission s'est récemment prononcée[146].

Plusieurs cas ont aussi été documentés dans les dernières années où des employés ont été soumis par l'employeur à des mesures intrusives de surveillance collectant des renseignements personnels grâce à des dispositifs technologiques numériques[147]. Cela s'accompagne d'une collecte inédite de données quantitatives sur la performance, mais aussi sur les comportements

---

141 Charte, art. 1.

142 Charte, art. 3.

143 Charte, art. 44.

144 Voir Michel FOUCAULT, *Surveiller et punir*, Paris, Gallimard, 1975; Madison VAN OORT, « The Emotional Labor of Surveillance: Digital Control in Fast Fashion Retail », (2019) 45-7-8 *Critical Sociology* 1168.

145 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Mémoire à la Commission de l'économie et du travail de l'Assemblée nationale sur le projet de loi nº 176, Loi modifiant la Loi sur les normes du travail et d'autres dispositions législatives*, (Cat. 2.412.86.5), 2018, p. 2 [En ligne]. https://www.cdpdj.qc.ca/storage/app/media/publications/memoire_PL_176_LNT.pdf; Judy FUDGE, « The Limits of Good Faith in the Contract of Employment: From *Addis* to *Vorvis* to *Wallace* and Back Again? » (2007) 32 *Queen's L.J.* 529, 530; *Evans* c. *Teamsters Local Union No. 31*, [2008] 1 RCS 661, par. 93.

146 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 11, p. 22. Voir également Amy TRAUB, *Discredited: How employment credit checks keep qualified workers out of a job*, Demos, 3 février 2014, [En ligne]. https://www.demos.org/research/discredited-how-employment-credit-checks-keep-qualified-workers-out-job

147 Voir Alexandra MATEESCU et Aiha NGUYEN, *Workplace Monitoring & Surveillance*, Data & Society, (février 2019), [En ligne]. https://datasociety.net/wp-content/uploads/2019/02/DS_Workplace_Monitoring_Surveillance_Explainer.pdf

et personnalités des employés[148]. Dans la mesure où les employés n'ont pas accès aux données enregistrées pas plus qu'à leur utilisation, cette pratique renforce l'asymétrie des forces entre employeurs et employés et nuit à leur capacité de lutter contre la discrimination[149]. Si la résistance individuelle et collective contre la surveillance est toujours possible, la précarisation du travail et la sophistication des outils de surveillance la rendent de plus en plus compliquée[150].

La surveillance constante, quand elle survient en milieu de travail[151], compromet aussi le droit à des conditions de travail justes et raisonnables et qui respectent sa santé, sa sécurité et son intégrité physique[152]. Pour les employeurs, le recours accru à des technologies de surveillance numérique répond à un intérêt d'augmentation de l'efficacité, de la production et de l'innovation. Pour les employés, en plus d'une intrusion toujours plus importante de la vie privée, cette surveillance peut avoir de nombreux effets délétères sur la santé physique et psychologique. En effet, la soumission à des impératifs de performance suivie électroniquement peut donner lieu à des risques accrus de blessures[153], à des comportements dangereux pour soi et le public[154], à

---

148 *Id.*

149 Joelle GAMBLE, « The Inequalities of Workplace Surveillance », *The Nation*, 3 juin 2019, [En ligne]. https://www.thenation.com/article/archive/worker-surveillance-big-data/. Dans les cas où ces données feraient l'objet d'un traitement algorithmique, cela ajouterait à l'opacité et pourrait encore davantage porter préjudice à l'employé

150 Dan CLAWSON et Mary Ann CLAWSON, « IT Is Watching : Workplace Surveillance and Worker Resistance » (2017) 26:2 *New Labor Forum* 62, [En ligne]. https://journals.sagepub.com/doi/abs/10.1177/1095796017699811; Kirstie Ball, « Workplace surveillance : an overview » (2010) 51:1 *Labor History* 87, [En ligne]. https://www.tandfonline.com/doi/abs/10.1080/00236561003654776?journalCode=clah20

151 COMMISSION DE L'ÉTHIQUE EN SCIENCE ET EN TECHNOLOGIE, *Les effets de l'intelligence artificielle sur le monde du travail : Document de réflexion*, Québec, 2019, p. 26 [En ligne]. https://www.ethique.gouv.qc.ca/assets/documents/IA_travail/CEST_effets_intelligence_artificielle_travail_A.pdf

152 Charte, art. 46. Pour un exemple d'application à un litige mettant en case l'utilisation d'un système de surveillance, voir *Centre intégré universitaire de santé et de services sociaux du Nord-de-l'Île-de-Montréal* c. *Jobin*, 2017 QCCS 1583.

153 Ifeoma AJUNWA, Kate CRAWFORD et Jason SCHULTZ, « Limitless Worker Surveillance » (2017) 105 *California Law Review* 735, [En ligne]. https://mronline.org/wp-content/uploads/2017/12/3Ajunwa-Schultz-Crawford-36.pdf

154 Par exemple, des camionneurs dont les mouvements sont surveillés ne respectent pas les limites de vitesse, ne prennent pas de pause et continuent à rouler malgré la fatigue. Voir Karen E. C. LEVY, « The Contexts of Control: Information, Power, and Truck-Driving Work », (2015) 31-2 *Inf. Soc.* 160-174, DOI : 10.1080/01972243.2015.998105; Hayley. PETERSON, , « 'We sped like crazy': Amazon delivery drivers say they feel pressure to drive dangerously, urinate in bottles, and sprint on the job », *Business Insider* (12 septembre 2018), [En ligne]. https://www.businessinsider.com/amazon-delivery-drivers-say-they-speed-urinate-in-bottles-2018-9.

une augmentation du niveau de stress au travail[155], etc. La surveillance numérique des consommateurs peut aussi mener à des pertes de revenus pour les employés et à une augmentation de leur précarité[156]. Par exemple, basée sur les données de consommation et de trafic, la génération automatisée d'horaires de travail est utilisée dans les secteurs du service et du commerce de détail alors qu'ils sont constitués par une main-d'œuvre précaire, féminine et racisée[157].

Notons que la pandémie risque de stimuler le recours à des outils de surveillance des employés en télétravail[158] et de surveillance des données biométriques et des comportements des employés[159], augmentant d'autant les risques d'atteintes aux droits.

Une multitude de dispositifs numériques sont utilisés pour surveiller les employés à distance. Cela inclut les logiciels qui permettent de surveiller les activités à l'ordinateur : suivi de l'utilisation d'Internet et des pages consultées, enregistrement des frappes au clavier, suivi des courriels, etc[160]. Depuis la pandémie de COVID-19 où le recours au télétravail s'est imposé, la demande pour de tels logiciels de surveillance à distance aurait crû de façon marquée[161]. La

---

155 Jamie WOODCOCK, « As a call centre worker I saw how employees are stripped of their rights », *The Guardian* (16 février 2017), [En ligne]. https://www.theguardian.com/careers/2017/feb/16/as-a-call-centre-worker-i-saw-how-employees-are-stripped-of-their-rights; M. VAN OORT, préc., note 144.

156 Dans le commerce du détail, la surveillance des consommateurs, que ce soit par l'enregistrement de données sur les habitudes de consommation ou par le suivi par Bluetooth, facilite de nouvelles formes de contrôle sur les employés et la réduction de leur pouvoir relatif. Voir Solon BAROCAS et Karen LEVY, « What Customer Data Collection Could Mean for Workers », *Harvard Business Review* (14 mai 2018), [En ligne]. https://hbr.org/2016/08/the-unintended-consequence-of-customer-data-collection

157 M. VAN OORT, préc., note 144. Des logiciels de paies automatisées permettent aussi de renvoyer automatiquement des employés à la maison en fonction des baisses des ventes, ce qui donne lieu à des pertes imprévues de revenus et facilite le vol de salaire. Voir J. GAMBLE, préc., note 149. Amazon utilise un logiciel qui piste et licencie automatiquement les employés d'entrepôt qui ne rencontrent pas les standards de productivité. Voir Colin LECHER, « How Amazon automatically tracks and fires warehouse workers for 'productivity' », *The Verge* (25 avril 2019), [En ligne]. https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations

158 Voir A. MATEESCU et A. NGUYEN préc., note 148; Sara MORRISON, « Just because you're working from home doesn't mean your boss isn't watching you », *Vox,* 2 avril 2020, [En ligne]. https://www.vox.com/recode/2020/4/2/21195584/coronavirus-remote-work-from-home-employee-monitoring

159 Voir N. CHYI, préc., note 17; J. VINCENT, préc., note 17.

160 Il s'agit de « flagging tools » qui ne permettent généralement pas une surveillance directe d'un humain sur un autre. Il s'agit plutôt de systèmes automatisés qui rapportent des comportements « suspects ». Voir A. MATEESCU et A. NGUYEN, préc., note 148.

161 S. MORRISON, préc., note 158.

pandémie est aussi l'occasion pour des entreprises d'implanter des mesures de surveillances technologiques qui analysent les données biométriques et les comportements des employés : caméras infrarouges pour mesurer la température corporelle, applications où les employés doivent rapporter leur état de santé, caméras utilisant la réalité augmentée et l'intelligence artificielle pour faire respecter les mesures de distanciation, etc.[162] Comme le note Zuboff, le milieu de travail est « l'endroit où les technologies invasives sont normalisées au sein de populations d'employés captifs[163] ». [Notre traduction.]

Par exemple, au Québec, Vidéotron Affaires offre depuis peu aux employeurs un bracelet visant à assurer le respect de la distanciation physique entre les employés en les avertissant par vibrations en cas de trop grande proximité, mesurée par la technologie Bluetooth[164]. Vidéotron précise que le produit a été développé de manière éthique et dans le respect de la vie privée. L'entreprise explique qu'elle n'a pas accès aux données et que les bracelets sont liés à des « identifiants anonymes ». Or, le dispositif enregistre les interactions et l'employeur connaît l'identité du porteur du bracelet. La protection de la vie privée de l'employé ne dépend donc que de la bonne volonté de l'employeur, sans garantie de protection du droit à la vie privée.

Le contexte social contemporain est en somme marqué par la production, la collecte et l'utilisation de volumes massifs de données d'une diversité inédite sur les personnes. Le développement de nouvelles technologies de l'information participe ainsi à l'érosion de la frontière entre les domaines public et privé qui pose de nouveaux défis en matière de protection des renseignements personnels. Nous avons vu que ces données sont des ressources centrales pour la surveillance à laquelle sont exposées les personnes dans leur vie quotidienne. Situer l'analyse du projet de loi à la lumière de ces éléments du contexte social permet de prendre la mesure des intérêts conflictuels et des risques associés à la collecte et à l'utilisation des renseignements personnels afin de proposer des modifications législatives adaptées à l'évolution des nouvelles technologiques et des enjeux sociaux qui y sont rattachés. Cela permet également d'inscrire la question de la protection des renseignements personnels dans le

---

162 N. CHYI, préc., note 17; J. VINCENT, préc., note 17.

163 S. ZUBOFF, préc., note 35.

164 VIDÉOTRON AFFAIRES, « Bracelet Radius », [En ligne]. https://videotron.com/affaires/p/produits-solutions/mobilite/appareils-accessoires/bracelet-radius/A-psku13550128f#/

cadre plus large et structurant du droit au respect de sa vie privée en interaction avec l'ensemble des droits et libertés énoncés à la Charte. On peut ainsi considérer, entre autres, les effets discriminatoires que peuvent entraîner la collecte et l'utilisation de données numériques par des acteurs publics et privés sur des groupes protégés en vertu de la Charte.

2 LES DROITS ET LIBERTÉS EN CAUSE DANS LA COLLECTE ET L'UTILISATION DES RENSEIGNEMENTS PERSONNELS

La protection des renseignements personnels, principal objet du projet de loi proposé, participe du droit au respect de sa vie privée garanti par la Charte[165]. Or, l'observation des travaux parlementaires récents ayant trait à la protection des renseignements personnels, entre autres ceux portant sur le projet de loi nº 53 concernant les agents d'évaluation de crédit et ceux portant sur les applications de notification de contact, nous porte à croire que peu d'intervenants tiennent compte de cet ancrage quasi constitutionnel. Cela étant, il nous apparaît essentiel de rappeler la source du caractère prééminent de la protection des renseignements personnels en droit québécois. En effet, comme l'a indiqué la Commission à l'égard du harcèlement psychologique :

> [L] es normes véhiculées par la Charte sont quasi constitutionnelles, c'est-à-dire qu'elles doivent prévaloir sur les considérations traitées par d'autres législations. Par conséquent, la Commission estime que lorsque d'autres instances traitent des cas de harcèlement sexuel selon leur juridiction, elles sont tenues de prendre en compte les droits prévus par la Charte, comme le droit au respect de sa dignité et le droit à l'égalité.[166] [Nous soulignons.]

Nous sommes d'avis que cette approche qui permet de renforcer la protection des droits devrait également prévaloir en matière de protection des renseignements personnels.

---

165 Charte, art. 5.

166 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 145, p. 45-46, citant COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Commentaires relatifs à la consultation portant sur le rapport de mise en œuvre du Plan d'action gouvernemental en matière d'agression sexuelle*, Aurélie Lebrun, Ariane Roy LeFrançois, Me Karina Montminy et Me Sophie Papillon, (Cat. 2.115.56), 2015, p. 30 [En ligne]. https://cdpdj.qc.ca/storage/app/media/publications/commentaires_plan_action_agression_sexuelle.pdf

Nous traiterons dans un premier temps du droit au respect de sa vie privée (section 2.1) pour aborder ensuite les autres droits qui peuvent mis en cause par la collecte et l'utilisation des données (section 2.2).

2.1 Le droit au respect de sa vie privée

Le droit au respect de sa vie privée a des sources multiples (2.1.1) qui lui confèrent une place spécifique en droit québécois (2.1.2). Il soulève par ailleurs des enjeux particuliers en ce qui a trait aux enfants et aux jeunes (2.1.3).

2.1.1 Les sources juridiques de la protection des renseignements personnels

La Cour suprême a relevé le lien qui existe entre la protection des renseignements personnels et le droit au respect de sa vie privée :

> [L]'objectif de fournir à une personne un certain droit de regard sur les renseignements personnels la concernant est intimement lié à son autonomie, à sa dignité et à son droit à la vie privée, des valeurs sociales dont l'importance va de soi.[167]

La Cour d'appel du Québec fait du contrôle sur les renseignements personnels un élément central du droit au respect de sa vie privée :

> Le droit à la vie privée peut se définir comme le droit d'un individu de déterminer lui-même quand, comment et dans quelle mesure il diffusera des renseignements personnels le concernant. Il protège ainsi une sphère d'autonomie individuelle.[168]

Si la notion de vie privée échappe à toute définition formelle en droit canadien[169], la Cour suprême en a esquissé les contours : celle-ci s'exprime à la fois en termes de lieux, d'intégrité physique et d'information, l'aspect informationnel de la vie privée se rapportant à la confidentialité, au contrôle sur l'accès et l'utilisation ainsi qu'à l'anonymat[170]. La Cour d'appel du

---

167 *Alberta (Information and Privacy Commissioner)* c. *Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401*, 2013 CSC 62, par. 24.

168 *9179-3588 Québec inc. (Institut Drouin)* c. *Drouin*, 2013 QCCA 2146, par. 51.

169 *Godbout* c. *Longueuil (Ville)*, [1997] 3 R.C.S. 844, par. 98 citant *Valiquette* c. *The Gazette (division Southam Inc.)*, [1996] J.Q. nº 445, 1996 CanLII 6004, par. 27 (QC C.A.).

170 *R.* c. *Spencer*, 2014 CSC 43, par. 35, 38 et 40.

Québec, pour sa part, identifie comme composantes du droit au respect de sa vie privée le droit à l'anonymat et à l'intimité, le droit à l'autonomie dans l'aménagement de sa vie personnelle et familiale ainsi que le droit au secret et à la confidentialité[171].

La protection des renseignements personnels a trait à l'aspect informationnel du droit au respect de sa vie privée et, dans la nomenclature de la Cour d'appel, à son aspect du droit au secret et à la confidentialité[172].

Le fait que la notion de vie privée ne soit pas formellement définie en droit canadien[173] lui permet de s'adapter aux différents contextes, notamment aux développements technologiques[174].

Les sources internationales des droits de la personne ont fortement influencé le contenu des instruments nationaux de protection des droits de la personne du Canada[175] et en particulier la Charte québécoise[176].

171 *Valiquette* c. *The Gazette (division Southam Inc.),* préc., note 169, p. 9.

172 Marie-Annik GRÉGOIRE, « Atteintes à la réputation et à la vie privée », dans JurisClasseur Québec, *Personnes et famille*, coll. « Droit civil », fasc. 4, Montréal, LexisNexis, feuilles mobiles, 2010 (maj 2020), par. 14.

173 Voir *infra,* section 2.1.1.

174 M.-A. GRÉGOIRE, préc., note 172, par. 13.

175 William SCHABBAS, « Le Canada et l'adoption de la Déclaration universelle des droits de l'homme », (1998) 11:2 *Revue québécoise de droit international* 67, 68; Bruce PORTER et MARTHA JACKMAN, « Introduction : Advancing Social Rights in Canada » dans Bruce PORTER et Martha JACKMAN (dir.), *Advancing Social Rights in Canada*, Toronto, Irwin Law, 2014, p. 1, à la p. 6.

176 André MOREL, « La Charte québécoise : un document unique dans l'histoire législative canadienne », (1987) 21 *Revue juridique Thémis* 1 à la p. 17; Pierre BOSSET et Michel COUTU, « Acte fondateur ou loi ordinaire? Le statut de la *Charte des droits et libertés de la personne* dans l'ordre juridique québécois », *Revue québécoise de droit international*, hors-série, juin 2015.

La *Déclaration universelle des droits de l'homme*[177] ainsi que le *Pacte international relatif aux droits civils et politiques*[178], auquel le Québec s'est déclaré lié[179], garantissent tous deux le droit au respect de la vie privée. Dans son Observation générale nº 16 de 1988 consacrée à l'interprétation du droit au respect de la vie privée, le Comité des droits de l'homme indique :

> Le rassemblement et la conservation, par des autorités publiques, des particuliers ou des organismes privés, de renseignements concernant la vie privée d'individus sur des ordinateurs, dans des banques de données et selon d'autres procédés, doivent être réglementés par la loi. L'État doit prendre des mesures efficaces afin d'assurer que ces renseignements ne tombent pas entre les mains de personnes non autorisées par la loi à les recevoir, les traiter et les exploiter, et ne soient jamais utilisés à des fins incompatibles avec le Pacte. Il serait souhaitable, pour assurer la protection la plus efficace de sa vie privée, que chaque individu ait le droit de déterminer, sous une forme intelligible, si des données personnelles le concernant et, dans l'affirmative, lesquelles, sont stockées dans des fichiers automatiques de données, et à quelles fins. Chaque individu doit également pouvoir déterminer les autorités publiques ou les particuliers ou les organismes privés qui ont ou peuvent avoir le contrôle des fichiers le concernant. Si ces fichiers contiennent des données personnelles incorrectes ou qui ont été recueillies ou traitées en violation des dispositions de la loi, chaque individu doit avoir le droit de réclamer leur rectification ou leur suppression.[180]

Le développement des technologies de l'information a entrainé de nouvelles préoccupations à l'échelle internationale en ce qui concerne la protection des droits de la personne. Dès 1990, l'Assemblée générale des Nations Unies adoptait des principes directeurs enjoignant les États

---

177 Rés AG 217A (III), Doc off AG NU, 3e sess, supp. n °13, Doc NU A/810 (1948) 71, art. 12:

Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

178 19 décembre 1966, 999 RTNU 171 (entrée en vigueur le 23 mars 1976), art. 17 :

Article 17

1. Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.

2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

179 Arrêté en conseil 1438-76 du 21 avril 1976 concernant la ratification du Pacte international relatif aux droits économiques, sociaux et culturels, du Pacte international relatif aux droits civils et politiques, du Protocole facultatif se rapportant aux droits civils et politiques, ainsi que la signature par Ottawa et les provinces d'une entente concernant les modalités de et le mécanisme de participation de ces dernières à la mise en œuvre des instruments internationaux, [En ligne].
http://www.mrif.gouv.qc.ca/document/spdi/fonddoc/FDOC_arret_1824_AC_1438-76.pdf

180 COMITÉ DES DROITS DE L'HOMME, *Observation générale nº 16 : article 17 (Droit au respect de la vie privée)*, Doc. N. U. HRI\GEN\1\Rev.1 (1994).

membres à réglementer le recours à des fichiers informatisés contenant des données à caractère personnel[181].

En 2013, l'Assemblée générale adoptait une résolution dans laquelle elle affirme que les droits dont les personnes jouissent hors ligne doivent être protégés en ligne et invite tous les États :

> […] b) À prendre des mesures pour faire cesser les violations de ces droits et à créer des conditions qui permettent de les prévenir, notamment en veillant à ce que la législation nationale applicable soit conforme aux obligations que leur impose le droit international des droits de l'homme ;
>
> c) À revoir leurs procédures, leurs pratiques et leur législation relatives à la surveillance et à l'interception des communications, et à la collecte de données personnelles, notamment à grande échelle, afin de défendre le droit à la vie privée en veillant à respecter pleinement toutes leurs obligations au regard du droit international ;
>
> d) À créer des mécanismes nationaux de contrôle indépendants efficaces qui puissent assurer la transparence de la surveillance et de l'interception des communications et de la collecte de données personnelles qu'ils effectuent, le cas échéant, et veiller à ce qu'ils en répondent, ou à les maintenir en place s'ils existent déjà.[182]

En 2014, le Haut-Commissariat des Nations Unies aux droits de l'homme produisait un rapport dans lequel il indiquait notamment :

> Le droit international des droits de l'homme établit un cadre clair et universel pour la promotion et la protection du droit à la vie privée, y compris dans le contexte de la surveillance sur le territoire national et à l'extérieur, de l'interception des communications numériques et de la collecte de données personnelles. Les pratiques suivies par de nombreux États ont toutefois fait apparaître l'absence de législation nationale et/ou de mesures d'application des lois suffisantes, la faiblesse des garanties procédurales et l'inefficacité du contrôle, lesquelles ont tous contribué à ce qu'il n'y ait pas d'obligation de rendre des comptes pour les atteintes arbitraires ou illégales au droit à la vie privée.[183]

Notons par ailleurs que la *Convention relative aux droits de l'enfant* prévoit à son article 16 :

> 1. Nul enfant ne fera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa

---

181 *Principes directeurs pour la réglementation des fichiers personnels informatisés*, Res. A.G. 45/95 (14 décembre 1990).

182 *Le droit à la vie privée à l'ère du numérique*, Doc. N. U. A/RES/68/167 (18 décembre 2013).

183 *Le droit à la vie privée à l'ère du numérique*, préc., note 21.

> réputation. 2. L'enfant a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

À la suite d'une journée générale de discussion, le Comité des droits de l'enfant recommandait ce qui suit :

> 19. Les États devraient garantir la protection du droit de l'enfant au respect de sa vie privée en relation avec les médias numériques et les technologies de l'information et de la communication et mettre en place des garanties contre les violations sans restreindre de manière abusive le plein exercice des droits consacrés dans la Convention[184].

Pour sa part, en mars 2015, le Conseil des droits de l'homme a nommé un rapporteur spécial sur la vie à la privée dont le mandat est notamment :

> […] De recueillir les informations voulues, notamment sur les cadres internationaux et nationaux, les pratiques et expériences nationales, d'étudier les tendances, les évolutions et les problèmes en ce qui concerne le droit à la vie privée et de faire des recommandations afin d'en garantir la promotion et la protection, notamment eu égard aux défis que posent les nouvelles technologies »[185].

À l'instar du Haut-Commissaire aux droits de l'homme, nous sommes d'avis que le cadre actuel de la protection des renseignements personnels n'est pas suffisant pour garantir le droit au respect de sa vie privée inscrit dans le droit international et incorporé dans la Charte québécoise.

Rappelons que les dispositions de la Charte lient aussi bien les acteurs publics[186] que privés[187] et ses articles 1 à 38 jouissent d'une préséance sur les dispositions des lois du Québec qui y seraient contraires[188]. Comme la Cour suprême du Canada l'indique :

---

184 COMITÉ DES DROITS DE L'ENFANT, *Recommandations issues de la journée de débat général de 2014 sur les droits de l'enfant et les médias numériques*, Annexe III du Rapport du Comité des droits de l'enfant, Doc. N. U. A/71/41, 2014, par. 19.

185 *Le droit à la vie privée à l'ère du numérique*, Doc. N. U. A/HRC/28/L.27 (24 mars 2015), al. 4 (a).

186 Charte, art. 55.

187 *Godbout* c. *Longueuil (ville)*, préc., note 169, par. 93

188 Sous réserve d'une dérogation expresse : Charte, art. 52.

> En raison de son statut quasi constitutionnel [la Charte], je le rappelle, a préséance, dans l'ordre normatif québécois, sur les règles de droit commun.[189]

En outre, le droit au respect de sa vie privée est garanti par les articles 35 et suivants du *Code civil du Québec*. Ces articles constituent en fait une mise en œuvre des droits consacrés à la Charte, comme l'illustrent les commentaires du ministre de la Justice à propos de la réforme du Code civil en 1993 :

> Le principe qui fonde cet article [35] se trouve aux articles 4 et 5 de la Charte des droits et libertés de la personne.
>
> L'introduction de ce principe au Code civil était nécessaire pour permettre d'en aménager l'exercice dans les articles ultérieurs.[190]

Par ailleurs, le droit au respect de la vie privée est également reconnu comme un droit de la personnalité par le *Code civil du Québec*[191]. Il est donc incessible[192]. La Cour supérieure du Québec indique :

> [L] es droits de la personnalité sont extrapatrimoniaux, en ce qu'ils sont intransmissibles, incessibles, insaisissables et imprescriptibles. Les auteurs Deleury et Goubau écrivent, à propos de l'incessibilité :
>
> « … Ils sont par le fait même incessibles : ils ne peuvent faire l'objet, par convention, d'une cession ou d'une renonciation de façon définitive. »[193]

Ainsi, précise une auteure :

> [L]'usage des droits de la personnalité ne peut faire l'objet d'une convention à caractère patrimonial. Par exemple, un artiste pourra consentir à ce que son image soit utilisée à des fins commerciales, sans que le droit du titulaire ne change de nature; le droit à son image demeure extrapatrimonial et inhérent à sa personne. À ce titre, les droits de la

---

189 *De Montigny* c. *Brossard (Succession)*, 2010 CSC 52, par. 45.

190 MINISTRE DE LA JUSTICE, *Commentaires du Ministre de la Justice : Le Code civil du Québec*, t.1, Québec, Publications du Québec, 1993, p. 33.

191 *Code civil du Québec*, article 35 et s.

192 *Id.*, art. 3.

193 *Savard* c. *Curtin-Savard*, 2012 QCCS 3523, par. 50, citant Édith DELEURY et Dominic GOUBAU, *Le droit des personnes physiques*, 4^e^ éd., Éd. Yvon Blais, 2008, p. 81.

> personnalité ne sont ni cessibles, ni saisissables, ni transmissibles, ni prescriptibles, ni susceptibles de renonciation. Ils s'imposent à toute personne, quelle qu'elle soit.[194]

Par conséquent, les renseignements personnels, même agrégés, ne devraient pas être considérés comme une ressource exploitable[195]. Nous y reviendrons.

Le corpus formé par la Loi sur le public, par la Loi sur le privé et, dans une moindre mesure, par la *Loi concernant le cadre juridique des technologies de l'information*[196] constitue un aménagement de l'aspect informationnel du droit au respect de sa vie privée garanti par la Charte et repris par le Code civil. D'ailleurs, la Loi sur le privé réfère spécifiquement aux dispositions du Code civil :

> La présente loi a pour objet d'établir, pour l'exercice des droits conférés par les articles 35 à 40 du Code civil en matière de protection des renseignements personnels, des règles particulières à l'égard des renseignements personnels sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise au sens de l'article 1525 du Code civil.[197]

Comme nous l'avons mentionné plus haut, la notion de vie privée que garantit la Charte est cependant plus large que son aspect informationnel ou son aspect de secret et de confidentialité. Le fait de recueillir et d'utiliser des renseignements personnels est aussi susceptible de compromettre les autres aspects du droit au respect de sa vie privée. Il s'agit notamment de l'aspect de la vie privée qui protège la sphère d'autonomie personnelle. En effet :

> Il est maintenant acquis que « le droit à la vie privée comprend le droit de prendre des décisions fondamentalement personnelles sans influence externe indue », y compris de la part de l'État. Seront aussi incluses dans ce critère les décisions qui ont un effet déterminant sur la qualité même de la vie privée.[198]

---

194 Hélène GUAY, « Les droits de la personnalité », dans *Collection de droit 2019-2020*, École du Barreau du Québec, Volume 3 : Personnes successions, Éd. Yvon Blais, 2019, 53 à la p. 53.

195 Voir : Maxime JOHNSON, « Mégadonnées: le nouveau pétrole », ***L'actualité***, 11 mai 2017, [En ligne]. https://lactualite.com/lactualite-affaires/megadonnees-le-nouveau-petrole/, citant « Fuel for the future : Data is giving rise to a new economy: How is it shaping up? », *The Economist*, 6 mai 2017, [En ligne]. https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy

196 RLRQ, c. C-1.1 (ci-après « Loi sur le cadre technologique »).

197 Loi sur le privé, art. 1er.

198 M.-A. GRÉGOIRE, préc., note 172, par. 17 référant à *Godbout* c. *Longueuil (Ville)*, préc., note 169, par 68 et 98.

2.1.2 La spécificité du droit au respect de sa vie privée en droit québécois

Le droit au respect de sa vie privée est garanti par l'article 5 de la Charte québécoise, dont l'adoption précède la Charte canadienne[199].

Rappelons que ce droit bénéficie de la préséance accordée aux dispositions de la Charte sur les autres dispositions des lois du Québec, sous réserve d'une dérogation expresse[200]. Ainsi, selon la Cour d'appel du Québec, la Loi sur le public, à l'instar des autres lois concernant la protection des renseignements personnels[201], tire son « caractère législatif fondamental » de « son rattachement à certains droits fondamentaux protégés par la *Charte des droits et libertés de la personne* [202] en particulier le droit au respect de sa vie privée.

Cependant, comme la Commission l'a déjà rappelé[203], le droit au respect de la vie privée n'est pas absolu. D'une part, la personne concernée peut valablement y renoncer. Pour être valide, une renonciation aux droits et libertés protégés par les Chartes doit cependant être « claire, non équivoque, éclairée, libre et volontaire puisqu'elle ne saurait se présumer »[204].

D'autre part, l'article 9.1 de la Charte prévoit une disposition justificative que le législateur ou une personne privée pourrait, selon les circonstances, invoquer en cas de violation des libertés et droits fondamentaux, consacrés aux articles 1 à 9. Cette disposition se lit comme suit :

---

199 *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, R.-U., c. 11)]. La plupart des dispositions de la Charte canadiennes sont entrées en vigueur en 1982 alors que celles de la Charte québécoise l'ont été en 1976.

200 Charte, art. 52.

201 *H.J. Heinz du Canada Ltée* c. *Canada (P. G.),* 2006 CSC 13, par. 28 ; *Lavigne* c. *Canada (Commissaire aux langues officielles)*, 2002 CSC 53, par 24 ; *Dagg* c. *Canada (Ministre des Finances)*, [1997] 2 R.C.S. 403, par. 65-66.

202 *Conseil de la magistrature du Québec* c. *Québec (Commission d'accès à l'information)*, 2000 CanLII 11305, [2000] R.J.Q 638 (C.A.), par. 50 cité dans Henri BRUN, « Le droit du public à l'information politique : un droit constitutionnel aux ancrages multiples » dans BARREAU DU QUÉBEC (dir.), *Développements récents en droit de l'accès à l'information 2005*, vol. 233, Cowansville, Yvon Blais, 91, p. 93.

203 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 21, p. 9; COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 11, p. 313, p. 4; COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE JEUNESSE, préc., note 13, p. 311, p. 4; COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 14, p. 16.

204 Christian BRUNELLE et Mélanie SAMSON, « Les limites aux droits et libertés » dans Collection de droit 2019-2020, École du Barreau du Québec, vol. 8, *Droit public et administratif*, Cowansville, Éditions Yvon Blais, 2019, 96 à la p. 99 [renvois omis.]

> Les libertés et droits fondamentaux s'exercent dans le respect des valeurs démocratiques, de la laïcité de l'État, de l'ordre public et du bien-être général des citoyens du Québec.
>
> La loi peut, à cet égard, en fixer la portée et en aménager l'exercice.

La détermination de la conformité à la Charte des atteintes au droit au respect de la vie privée commande un examen minutieux[205]. La démarche à suivre est bien définie et largement confirmée par les tribunaux[206]. La Cour suprême a ainsi établi que « pour se prévaloir de l'article 9.1, le gouvernement doit démontrer que la loi restrictive n'est ni irrationnelle ni arbitraire et que les moyens choisis sont proportionnés au but visé »[207].

Le droit au respect de sa vie privée garanti par la Charte québécoise s'apparente au droit dérivé de la protection contre les fouilles, les perquisitions ou les saisies abusives garanti par la *Charte canadienne des droits et libertés*[208]. En effet, la Cour suprême reconnaît depuis longtemps que le respect de la vie privée est l'objectif promu par l'article 8 de la Charte canadienne[209]. Cependant, selon la Cour suprême du Canada, pour faire valoir ce droit, le demandeur doit démontrer une attente subjective de vie privée objectivement raisonnable[210]. La Cour précise :

> Pour se réclamer de la protection de l'art. 8, le demandeur doit d'abord démontrer qu'il pouvait raisonnablement compter sur le respect de sa vie privée à l'égard de l'objet de la fouille ou de la perquisition, en d'autres termes, qu'il s'attendait subjectivement à ce que l'objet de la fouille soit privé et que cette attente était objectivement raisonnable. Le caractère raisonnable de l'attente d'une personne au respect de sa vie privée dépend de « l'ensemble des circonstances ». C'est la méthode à employer pour décider s'il existe une attente raisonnable en matière de respect de la vie privée à l'égard d'une conversation par message texte.[211]

---

205 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 13.

206 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Mémoire à la Commission des institutions de l'Assemblée nationale concernant le Projet de loi nº 60, Charte affirmant les valeurs de laïcité et de neutralité religieuse de l'État ainsi que d'égalité entre les femmes et les hommes et encadrant les demandes d'accommodement*, (Cat. 2.113-2.13), 2013, p. 29.

207 *Ford* c. *Québec (Procureur général)*, [1988] 2 R.C.S. 712, 1988 CanLII 19, par. 63 (CSC).

208 Préc., note 199.

209 *Hunter* c. *Southam inc*., [1984] 2 R.C.S. 145, *R.* c. *Dyment,* [1988] 2 R.C.S. 217 à la p. 426*; R*. c. *Duarte*. [1990] 1 R.C.S. 30 à la p. 43.

210 *R.* c. *Marakah*, 2017 CSC 59, par. 12.

211 *Id.*, par. 10 [renvois omis].

Comme l'indiquent les auteurs Benyekhlef et Déziel, « [s] ans la démonstration de l'existence de cette attente, toute fouille, saisie ou perquisition ne sera pas considérée comme visée par l'article 8 de la Charte [canadienne] »[212]. Le droit au respect de sa vie privée n'est donc pas explicitement consacré dans la Charte canadienne. Il est reconnu indirectement et sous réserve de démontrer une attente raisonnable à son égard.

La Charte québécoise comporte également, à l'article 24.1, une protection contre les saisies, les perquisitions et les fouilles abusives et cette disposition devrait recevoir la même interprétation que l'article 8 de la Charte canadienne[213].

Or, la Charte québécoise comporte aussi une disposition spécifique garantissant le droit au respect de sa vie privée[214]. De l'avis de la Commission, l'article 5 de la Charte devrait être interprété différemment de son article 24.1, notamment parce que le premier se trouve dans le chapitre consacré aux « Droits et libertés fondamentaux » alors que le second se trouve dans le chapitre des « Droits judiciaires ». Il faut donc user de circonspection avant d'appliquer les notions de vie privée élaborées en contexte judiciaire en vertu de l'article 8 de la Charte canadienne[215] à l'article 5 de la Charte québécoise, notamment la notion d'attente raisonnable de vie privée. Dans une décision concernant la mise en œuvre de l'article 5 de la Charte, la Cour suprême indique d'ailleurs :

> On aurait donc tort de fixer la portée du droit à la vie privée entre citoyens sur la seule base de la jurisprudence entourant l'art. 8 [de la Charte canadienne]. Bien que je souscrive aux définitions fonctionnelles de vie privée adoptées par notre Cour […], il me semble que le droit à la vie privée peut avoir une étendue différente en droit privé.[216]

---

212 Karim BENYEKHLEF et Pierre-Luc DÉZIEL, *Le droit à la vie privée en droit québécois et canadien*, Montréal, Éd. Yvon Blais, 2018, p. 79.

213 *Comité paritaire de l'industrie de la chemise* c. *Potash*; *Comité paritaire de l'industrie de la chemise* c. *Sélection Milton*, [1994] 2 RCS 406 à la p. 413.

214 Charte, art. 5.

215 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, « Oser la transparence et savoir la doser : à la recherche d'un équilibre, présentation faite par Philippe-André TESSIER, président, à l'occasion du colloque organisé par la Chaire sur la démocratie et les institutions parlementaires de l'Université Laval intitulé « La transparence réussie : enjeux et limites », Québec, 14 novembre 2019.

216 *Aubry* c. *Éditions Vice-Versa inc*., [1998] 1 R.C.S. 591, par. 9.

La Commission est d'avis que la mise en garde est valable pour l'ensemble des applications du droit au respect de sa vie privée qui ne relèvent pas de l'application de l'article 24.1 de la Charte québécoise.

Par ailleurs, la professeure Teresa Scassa souligne l'importance de considérer le droit au respect de sa vie privée comme un droit fondamental :

> Une approche de la vie privée fondée sur les droits de la personne permet non seulement de reconnaître le droit fondamental au respect de sa vie privée, mais reconnaît également ses interactions avec le droit d'exercer ses autres droits et libertés avec autonomie et dignité. En outre, le droit fondamental au respect de sa vie privée doit être supporté par une législation qui le rend effectif et réalisable.
>
> Une approche de la vie privée fondée sur les droits de la personne reconnaît non seulement un droit fondamental à la vie privée, mais reconnaît également l'interdépendance entre la vie privée et le droit des personnes d'exercer leurs autres droits et libertés avec autonomie et dignité. De plus, le droit à la vie privée doit être soutenu par une législation qui rend le droit effectif et réalisable.[217] [Notre traduction.]

Le fait que le droit au respect de sa vie privée soit spécifiquement reconnu par la Charte permet le recours à cette approche.

De plus, rappelons que le droit au respect de sa vie privée est, en vertu du *Code civil du Québec*, un droit de la personnalité[218], et qu'à ce titre, les renseignements personnels des Québécois ne devraient pas être considérés comme une ressource exploitable[219]. Cette situation se distingue de celles des États-Unis, par exemple, où le droit au respect de sa vie privée n'est pas constitutionnalisé[220] et où l'État accorde une protection limitée aux informations dites sensibles[221] sur une base sectorielle[222] seulement. Conséquemment, le filet de protection

---

217 Teresa SCASSA, « A Human Rights-Based Approach to Data Protection in Canada", dans Elizabeth DUBOIS et Florian MARTIN-BARIBEAU, *Citizenship in a Connected Canada: A research Policy Agenda*, Ottawa, University of Ottawa Press, 2020,

218 *Code civil du Québec*, art. 3.

219 M. JOHNSON, préc., note 195.

220 Avner LEVIN et Mary Jo NICHOLSON, « Privacy Law in the United States, the Eu and Canada: The Allure of Middle Ground », [2005] 2:2 *University of Ottawa Law & Technology Journal* 357, p. 367.

221 Paul M. SCHWARTZ, « The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures », [2013] Harvard L. R. 1965, 1978.

222 *Id.*, 1974-1975.

de la vie privée dans ce pays est quelque peu décousu et il est difficile de définir une règle générale applicable à tous les secteurs et à tous les acteurs[223]. Les entreprises qui œuvrent dans des secteurs qui ne sont pas encore réglementés ne sont donc pas contraintes par des règles concernant le respect de sa vie privée[224].

Ce faisant, le Québec ne devrait pas être confronté, comme d'autres États le sont, au dilemme politique entre la protection du droit au respect de sa vie privée comme un droit fondamental ou la protection des renseignements personnels comme marchandises[225], le choix ayant été fait au moment de l'adoption de la Charte.

2.1.3 Le droit au respect de sa vie privée des personnes mineures

À l'instar des personnes majeures, les personnes mineures jouissent de tous les droits prévus à la Charte, incluant le droit au respect de sa vie privée. Tous les aspects du droit au respect de la vie privée détaillés plus haut jouent un rôle important dans leur développement[226]. Les personnes mineures jouissent aussi du droit « à la protection, à la sécurité et à l'attention que [leurs] parents ou les personnes qui en tiennent lieu peuvent lui donner. »[227]

Pour établir un équilibre entre « les responsabilités des parents et le respect qu'on reconnaît maintenant à l'enfant, en tant que personne à part entière »[228], le droit québécois accorde aux personnes mineures un « accès graduel à l'autonomie[229]. »

La quête de cet équilibre mérite un examen attentif dans le cas de la protection des renseignements personnels et du respect de la vie privée[230]. Par exemple, les enfants sont

---

223 A. LEVIN et M.J. NICHOLSON, préc., note 220, 361.

224 P.M. SCHWARTZ, préc., note 221, 1978.

225 J. R. REIDENBERG, préc., note 24.

226 UNICEF, préc., note 84, p. 9; *A.B. c. Bragg*, 2012 CSC 46, par. 17.

227 Charte, art. 39.

228 Claire BERNARD, « Les droits de l'enfant, entre la protection et l'autonomie », dans Lucie LAMARCHE et Pierre BOSSET (dir.), *Des enfants et des droits*, Québec, Presses de l'Université Laval, 1997, p. 30.

229 *Id.*, p.26.

230 UNICEF, préc., note 84, p. 4.

particulièrement susceptibles à la publicité ciblée[231] et c'est donc à juste titre que les titulaires de l'autorité parentale pourraient vouloir limiter la collecte et l'utilisation de renseignements permettant de les profiler et les cibler. Néanmoins, les mesures de protection mises en place peuvent devenir des mécanismes de surveillance et de contrôle néfastes[232].

Il faut de plus souligner que les renseignements partagés par les parents au sujet de leurs enfants, notamment sur les réseaux sociaux, sont susceptibles de porter atteinte à leur droit au respect de sa vie privée dans le moment présent ou dans le futur[233]. Cela peut aussi entraîner des atteintes à d'autres droits des personnes mineures. Par exemple, une photo ou un article de blogue peut faire de son sujet la cible de cyberintimidation[234], risquant ainsi de nuire au droit à la sauvegarde de sa dignité, de sa sûreté et de son intégrité psychologique. Dans des cas graves, des photos d'enfants partagés par leurs parents ont aussi été détournées et retrouvées sur des sites de pornographie juvénile[235]. Les informations partagées au sujet de personnes mineures permettent aussi aux entreprises de dresser un profil à leur sujet[236]. Un tel profilage peut porter atteinte à leur droit à la liberté[237] ainsi qu'à l'égalité[238]. Par exemple, Bailey et Steeves notent que le profilage des jeunes en ligne tend à renforcer les stéréotypes fondés sur le genre[239].

Il est donc essentiel que les régimes de protection des renseignements personnels portent une attention particulière aux besoins et aux droits des enfants. La chercheuse en droit Milda Macenaite le formule ainsi:

---

231 *Id*., p. 12. La *Loi sur la protection du consommateur* le reconnaît d'ailleurs : RLRQ, c. P-40.1, art. 248, 249.

232 Milda MACENAITE, « From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation », (2017) 19-5 *new media & society* 765, 773; UNICEF, préc., note 84, p. 4.

233 UNICEF, préc., note 84, p. 9; OPTION CONSOMMATEURS, préc., note 85.

234 OPTION CONSOMMATEURS, *id.*, p. 9-10; COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Commentaires sur le projet de loi nº 56, Loi visant à lutter contre l'intimidation et la violence à l'école*, Aurélie LEBRUN et Me Karina MONTMINY, (Cat. 2.412.117), 2012, p. 11-12.

235 OPTION CONSOMMATEURS*, id*., p. 5-6.

236 *Id*., p. 7.

237 Voir *infra*, section 2.2.3

238 Voir *infra*, section 2.2.2

239 J. BAILEY et V. STEEVES, préc., note 81, p. 2.

> Idéalement, la législation en matière de protection des données devrait protéger les enfants contre les risques d'atteinte à la vie privée, comme l'exploitation commerciale des données ou une mauvaise utilisation de celles-ci, les atteintes à la réputation, à l'identité, à la dignité et à l'intégrité, tout en augmentant les opportunités en ligne. Ceci requiert un cadre réglementaire qui impose des obligations légales aux gestionnaires de données et qui vise parallèlement à promouvoir l'autonomie des enfants tout en répondant aux besoins de ceux et celles qui requièrent plus de protection. [Notre traduction][240]

2.2 Les autres droits qui peuvent être mis en cause par la collecte des renseignements personnels

Si, comme nous l'avons mentionné à la section précédente, le cadre actuel de la protection des renseignements personnels n'est pas suffisant pour garantir le droit au respect de sa vie privée inscrit dans le droit international et incorporé dans la Charte québécoise, il l'est encore moins pour garantir les autres droits qui peuvent être affectés par la collecte et l'utilisation des renseignements personnels.

En effet, les droits de la personne sont indivisibles et interdépendants[241]. La communauté internationale a réaffirmé cette interdépendance à l'occasion de la Conférence mondiale sur les droits de l'homme en 1993 :

> Tous les droits de l'homme sont universels, indissociables, interdépendants et intimement liés. […][242]

Comme l'explique la Ligue des droits et libertés, « [l]'interdépendance des droits consiste à reconnaître que la réalisation d'un droit est intimement liée à celles des autres droits »[243].

C'est donc dire que le droit au respect de sa vie privée dépend de la réalisation des autres droits garantis par la Charte et vice-versa. De l'avis de la Commission, on doit donc, dans le cadre d'une démarche de modernisation de la législation visant la protection des

---

240 M. MACENAITE, préc., note 232, p. 769

241 *Gosselin* c. *Québec (P. G.)*, [1999] R.J.Q. 1033 (C.A.) p. 205 référant à la *Déclaration universelle des droits de l'homme*, préc., note 177.

242 CONFÉRENCE MONDIALE SUR LES DROITS DE L'HOMME, *Déclaration et programme d'action de Vienne*, Doc. N. U. A/CONF.157/23 (Vienne 14-25 juin 1993), art. 5.

243 LIGUE DES DROITS ET LIBERTÉS, *Ensemble, rétablissons les droits*, 2013, p. 1 [En ligne]. https://liguedesdroits.ca/wp-content/fichiers/retablissons-les-droits-fiches.pdf

renseignements personnels, considérer les autres droits qui peuvent être mis en cause par la collecte et l'utilisation des renseignements personnels. On pense notamment au droit à l'égalité, aux libertés fondamentales, aux droits politiques, aux droits judiciaires et au droit de vivre dans un environnement sain et respectueux de la biodiversité.

2.2.1 Le droit au respect de sa dignité, de son honneur et de sa réputation

L'article 4 de la Charte énonce que « toute personne a droit à la sauvegarde de sa dignité, de son honneur et de sa réputation ».

La Cour suprême fait une association similaire en ce qui concerne les droits garantis par la *Charte canadienne des droits et libertés*[244] :

> Bien qu'elle ne soit pas expressément mentionnée dans la Charte [canadienne], la bonne réputation de l'individu représente et reflète sa dignité inhérente, concept qui sous-tend tous les droits garantis par la Charte. La protection de la bonne réputation d'un individu est donc d'importance fondamentale dans notre société démocratique.[245]

Dans son sens ordinaire, le terme réputation désigne « la manière dont quelqu'un est connu, considéré dans un public » ou encore l'« opinion favorable ou défavorable pour quelqu'un, quelque chose »[246]. La notion de « réputation » se distingue de celle « d'honneur » parce que la première relève de l'opinion publique alors que la seconde est plus intime[247].

Le droit à la sauvegarde de la réputation est également étroitement lié au droit au respect de la vie privée, comme le révèle leur association dans plusieurs dispositions du *Code civil du Québec*[248]. Cela étant, les deux droits sont distincts :

---

244 Préc., note 199.

245 *Hill* c. *Église de Scientologie de Toronto*, [1995] 2 R.C.S. 1130, par. 120.

246 LAROUSSE, « Dictionnaire de français », s.v. « réputation », [En ligne]. https://www.larousse.fr/dictionnaires/francais/r%c3%a9putation/68543?q=r%c3%a9putation#67795

247 Hélène GUAY, « Les droits de la personnalité » dans Collection de droit 2019-20, École du Barreau du Québec, vol. 3, *Personnes et succession*, Cowansville, Éditions Yvon Blais, 2019, p. 53, à la p. 75.

248 L'article 3 du *Code civil du Québec* prévoit :

« 3. Toute personne est titulaire de droits de la personnalité, tels le droit à la vie, à l'inviolabilité et à l'intégrité de sa personne, au respect de son nom, de sa réputation et de sa vie privée.

> « Il est donc acquis que la sauvegarde de la réputation comme la protection de l'honneur et de la dignité sont inscrites au fronton des droits fondamentaux auxquels souscrit la collectivité canadienne. Il s'agit -là du respect sacro-saint de l'individu. Associée de près à la protection de la vie privée, la sauvegarde de la réputation ne partage pas la même fin même si les deux se rejoignent pour dresser un barrage contre l'altération publique de la personnalité de la victime. »[249] [Nous soulignons.]

L'usage qui est fait des renseignements personnels recueillis à propos d'une personne est susceptible de constituer une altération publique de sa personnalité et, par conséquent, peut affecter son droit à la sauvegarde de sa dignité, de son honneur et de sa réputation garanti par la Charte.

2.2.2 Le droit à l'égalité

L'article 10 de la Charte garantit le droit à l'égalité en ces termes :

> Toute personne a droit à la reconnaissance et à l'exercice, en pleine égalité, des droits et libertés de la personne, sans distinction, exclusion ou préférence fondée sur la race, la couleur, le sexe, l'identité ou l'expression de genre, la grossesse, l'orientation sexuelle, l'état civil, l'âge sauf dans la mesure prévue par la loi, la religion, les convictions politiques, la langue, l'origine ethnique ou nationale, la condition sociale, le handicap ou l'utilisation d'un moyen pour pallier ce handicap.
>
> Il y a discrimination lorsqu'une telle distinction, exclusion ou préférence a pour effet de détruire ou de compromettre ce droit.

Le fait de recueillir et d'utiliser des renseignements personnels est susceptible de compromettre ce droit. Le traitement automatisé des données, par le recours à l'intelligence artificielle, par exemple, est particulièrement inquiétant à cet égard.

En effet, comme le soulignait récemment la Commission, le recours à des systèmes d'intelligence artificielle, une forme très répandue de traitement automatisé, *a priori* neutre, peut

---

> Ces droits sont incessibles.
>
> Pour sa part, l'article 35 énonce :
>
> « 35. Toute personne a droit au respect de sa réputation et de sa vie privée.
>
> Nulle atteinte ne peut être portée à la vie privée d'une personne sans que celle-ci y consente ou sans que la loi l'autorise. »

249 *Lapierre* c. *Sormany*, 2012 QCCS 4190, par. 91.

compromettre le droit à l'égalité par la production de décisions influencées par des biais discriminatoires[250]. La Commission explique :

> Par exemple, des systèmes destinés à faciliter l'embauche de personnel, pourtant conçus sans volonté de créer des biais discriminatoires, se sont ainsi avérés avoir un effet disproportionnellement excluant pour certains groupes de personnes. Un système automatique de filtrage des candidatures, mis en place par une grande entreprise œuvrant dans le secteur des technologies, aurait, par exemple, développé un biais négatif à l'encontre des candidatures féminines. Un pointage plus faible aurait ainsi été attribué à celles-ci, les résultats émis par l'algorithme ayant reproduit les inégalités de genre déjà présentes dans les catégories d'emplois visés. Des résultats discriminatoires, produits par des outils technologiques utilisés sans intention malveillante, ont aussi été observés à l'encontre de personnes racisées dans l'utilisation d'outils de reconnaissance faciale, d'accès aux soins de santé ou de prédiction du risque de la récidive en matière criminelle. Des auteurs ont également documenté des effets discriminatoires involontaires liés à la condition sociale alors que d'autres soulignent que les [systèmes d'intelligence artificielle] pourraient avoir des effets préjudiciables à l'endroit d'autres groupes dans différents domaines.[251] [Renvois omis.]

La Commission notait alors qu'il importe d'évaluer les systèmes d'intelligence artificielle non pas uniquement en fonction de leurs objectifs ou des fins poursuivies, mais également en fonction de leurs résultats effectifs[252].

2.2.3 Les libertés fondamentales

La Cour suprême reconnaît que la notion de vie privée repose notamment sur l'autonomie des personnes :

> Étant l'expression de la personnalité ou de l'identité unique d'une personne, la notion de vie privée repose sur l'autonomie physique et morale — la liberté de chacun de penser, d'agir et de décider pour lui-même.[253]

Il apparaît que les notions de vie privée et de liberté se rejoignent dans la protection de l'autonomie personnelle. En effet, la Cour suprême décrit la liberté « comme l'absence de

---

250 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 13, p. 7-8.

251 *Id.*, p. 7.

252 *Id.*, p. 8.

253 *Dagg* c. *Canada (Ministre des Finances)*, préc., note 201, par. 65; Voir également *R.* c. *Dyment*, préc., note 209, p. 427.

coercition et la faculté de chacun de faire des choix fondamentaux dans la vie »[254]. Elle indique ailleurs :

> D'autre part, la liberté ne signifie pas simplement l'absence de toute contrainte physique. Dans une société libre et démocratique, l'individu doit avoir suffisamment d'autonomie personnelle pour vivre sa propre vie et prendre des décisions d'une importance fondamentale pour sa personne.[255]

C'est donc dire que la notion de liberté telle que reconnue par les articles 1 et 3 de la Charte converge avec l'aspect d'autonomie personnelle de droit au respect de sa vie privée.

De plus en plus de données sont générées par les individus, par leur utilisation d'outils numériques, notamment, et sont détenues et exploitées par d'autres[256]. Les chercheurs reconnaissent depuis longtemps que la collecte de ces données par les acteurs privés et publics a comme objectif ultime d'influencer le comportement des titulaires de ces données[257]. Cette influence peut avoir un impact sur l'autonomie personnelle et, par conséquent, la liberté de sa personne[258] et les autres libertés fondamentales, telles la liberté de conscience, la liberté de religion, la liberté, la liberté d'opinion, la liberté d'expression, la liberté de réunion pacifique et la liberté d'association[259]. En effet, plus on en sait sur une personne, plus il est facile de la contrôler[260]. En outre, la surveillance constante peut affecter l'intégrité psychologique des personnes, qui relève du droit à l'intégrité[261], et , quand elle survient en milieu de travail, peut

---

254 *Procureur général de la Nouvelle-Écosse* c. *Walsh*, 2002 CSC 83, par. 63.

255 *B. (R.)* c. *Children's Aid Society of Metropolitan Toronto*, [1995] 1 R.C.S. 315, par. 80.

256 Shoshana ZUBOFF, « Big Other: Surveillance Capitalism and the Prospect of an Information Civilization », (2015) 30:1 *Journal of Information* 75.

257 Spiros SIMITIS, « Reviewing Privacy in an Information Society », (1987) 135 *University of Pennsylvania Law Review* 707, 710; S. ZUBOFF, *id*.

258 Charte, art. 1er.

259 Notamment la liberté de conscience, la liberté de religion, la liberté d'opinion, la liberté d'expression, la liberté de réunion pacifique et la liberté d'association : Charte, art. 3.

260 Paul SCHWARTZ, « The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination », (1989) 37:4 *American Journal of Comparative Law* 675, 676.

261 Charte, art. 1er; *Québec (Curateur public)* c. *Syndicat national des employés de l'hôpital St-Ferdinand*, [1996] 3 R.C.S. 211, par. 95.

compromettre aussi le droit à des conditions de travail justes et raisonnables et qui respectent sa santé, sa sécurité et son intégrité physique[262].

2.2.4 Les droits politiques

La Charte garantit le droit de vote en ces termes :

> 22. Toute personne légalement habilitée et qualifiée a droit de se porter candidat lors d'une élection et a droit d'y voter.

La protection du droit de vote implique notamment l'accès aux informations nécessaires pour voter de façon éclairée[263]. La Cour suprême indique :

> Les élections n'ont de caractère juste et équitable que si tous les citoyens et citoyennes sont raisonnablement informés de tous les choix possibles et que l'on donne une possibilité raisonnable aux partis, aux candidats et aux candidates d'exposer leur position afin que le débat électoral ne soit pas dominé par ceux qui ont accès à des moyens financiers plus importants.[264]

Les révélations concernant le transfert des renseignements personnels de millions d'usagers sans leur consentement par Facebook à l'entreprise Cambridge Analytica[265], évoqué ci-dessus, mettent en cause le droit de vote[266]. Pour rappel, ces données étaient utilisées pour créer des profils psychologiques individuels qui pouvaient ensuite servir à cibler spécifiquement les individus en vue d'influencer leur comportement, notamment en matière électorale[267]. Les

---

262 Charte, art. 46; COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Surveillance par Caméra vidéo des lieux de travail : compatibilité avec la Charte*, Me Daniel CARPENTIER, (Cat. 2178.1), 1986, [En ligne]. https://cdpdj.qc.ca/storage/app/media/publications/camera.pdf ; Syndicat de l'enseignement de la région des Moulins et Commission scolaire des Affluents, 2018 QCTA 196; *Fraternité des policiers de Ville de Mont-Tremblant et Ville de Mont-Tremblant (grief syndical),* 2020 QCTA 183.

263 *Harper* c. *Canada (P. G.)*, 2004 CSC 33, au par. 71.

264 *Libman* c. *Québec (P. G.)*, [1997] 3 R.C.S. 569 au par. 47.

265 Caroline CADWALLAR et Emma GRAHAM-HARRISON, « Revealed : 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach »,, *The Guardian*, 17 mars 2018, [En ligne]. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

266 J. ISAAK et M. J. HANNA, préc., note 49.

267 James MCLEOD, « Canada's AggregateIQ broke Privacy law in Cambridge Analytica Scandal, probe finds", *Financial Post*, 26 novembre 2019, [En ligne]. https://financialpost.com/technology/canadas-aggregateiq-broke-privacy-law-in-cambridge-analytica-scandal-probe-find

mesures mises en place par l'entreprise pour influencer le vote contournent les règles entourant entre autres le financement des partis et des campagnes électorales[268].

Dans la foulée du scandale Cambridge Analytica, une enquête a été menée conjointement par le Commissariat à la protection de la vie privée du Canada et le Bureau du Commissaire à l'information et la protection de la vie privée de la Colombie-Britannique à propos des travaux d'AggragateIQ Data Services Ltd, une entreprise sise en Colombie-Britannique. Cette enquête a révélé que l'entreprise a contrevenu aux lois en matière de protection des renseignements personnels de la Colombie-Britannique et du Canada en fournissant des services à deux campagnes à l'occasion du référendum de 2016 sur l'appartenance du Royaume-Uni à l'Union européenne ainsi que lors des élections américaines de mi-mandat en 2014[269]. La CAI s'est aussi inquiétée des fuites de données personnelles dans le but de manipuler l'opinion publique lors de campagnes électorales[270]. C'est donc dire que les citoyens canadiens et québécois ne sont pas à l'abri de cette pratique. D'ailleurs, un recours collectif a été intenté en Ontario contre l'entreprise Facebook pour avoir partagé, sans leur consentement, les données de résidents canadiens avec Cambridge Analytica[271]. Notons que les Commissaires canadien et britanno-colombien ont dit regretter de ne pas avoir les pouvoirs nécessaires pour sanctionner la compagnie fautive[272].

2.2.5 Les droits judiciaires

La Charte garantit certains droits judiciaires, dont la protection contre les saisies, les perquisitions et fouilles abusives. L'article 24.1 de la Charte indique en effet que :

---

268 J. ISAAK et M. J. HANNA, préc., note 49, p. 58.

269 *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 d'AggregateIQ Date sevices Ltd*., 26 octobre 2019, [En ligne]. https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2019/lprpde-2019-004/

270 COMMISSION D'ACCÈS À L'INFORMATION, « Fuite de données personnelles de milliers d'utilisateurs de Facebook, 20 mars 2018, [en ligne]. https://www.cai.gouv.qc.ca/fuite-de-donnees-personnelles-de-milliers-dutilisateurs-de-facebook/

271 « Un recours collectif contre Facebool lancé au Canada », *Ici Radio-Canada*, 25 avril 2018, [en ligne.] https://ici.radio-canada.ca/nouvelle/1097411/recours-collectif-canadien-contre-geant-facebook; La demande introductive d'instance est disponible ici : https://kmlaw.ca/wp-content/uploads/2019/04/Fresh-as-Amended-Statement-of-Claim-amended-on-January-24-2019.pdf

272 J. MCLEOD, préc., note 267.

> Nul ne peut faire l'objet de saisies, perquisitions ou fouilles abusives.

Cette disposition, distincte du droit au respect de sa vie privée[273], protège notamment contre « les intrusions injustifiées de l'État dans [la] vie privée »[274]. Elle trouve application quand il existe une attente raisonnable de vie privée[275]. Comme nous l'avons indiqué, cette disposition devrait recevoir la même interprétation que l'article 8 de la Charte canadienne.[276].

La Cour suprême a convenu que « la surveillance électronique d'un particulier par un organe de l'État constitue une fouille, une perquisition ou une saisie abusive au sens de l'art. 8 de la Charte [canadienne] »[277]. Elle s'est opposée au fait que des agents de l'État puissent « braquer des caméras dissimulées sur des membres de la société, en tout temps et en tout lieu, à leur gré[278] » et s'est prononcée sur le recours aux nouvelles technologies à des fins de surveillance :

> [L] e droit général à la protection contre les fouilles, les perquisitions ou les saisies abusives garanti par l'art. 8 [de la Charte canadienne] doit évoluer au rythme du progrès technologique et, par conséquent, nous assurer une protection constante contre les atteintes non autorisées à la vie privée par les agents de l'État, peu importe la forme technique que peuvent revêtir les divers moyens employés[279].

Ainsi, la Cour suprême a reconnu qu'il existait une attente raisonnable de vie privée quant à un téléphone cellulaire[280], y compris les textos qui se trouvent sur un autre téléphone que celui de l'expéditeur[281], et quant aux ordinateurs personnels[282], même quand il est prêté par l'employeur[283].

---

273 Charte, art. 5; Voir infra, section 2.1.2.

274 *Hunter* c. *Southam,* préc., note 209, p. 160.

275 *R.* c. *M.(M.R.)*, [1998] 3 R.C.S. 393, par. 31.

276 Voir *infra*, la section 2.1.2.

277 *R. c. Duarte*, [1990] 1 R.C.S. 30, 1990 CanLII 150, p. 42-43 (CSC).

278 *R. c. Wong*, [1990] 3 R.C.S. 36, 1990 CanLII 56, p. 47 (CSC).

279 *R. c. Société TELUS Communications*, [2013] 2 R.C.S. 3, 2013 CanLII 16, par. 33 (CSC), citant *id*., p. 44.

280 *R.* c. *Fearon*, 2014 CSC 77.

281 *R.* c. *Marakah*, 2017 CSC 59.

282 *R.* c. *Morelli*, 2010 CSC 8.

283 *R.* c. *Cole*, 2012 CSC 53.

C'est donc dire que lorsque l'État recueille des données produites par l'activité en ligne, et ce, sans mandat de perquisition et sans obtenir l'autorisation des citoyens, il est susceptible de contrevenir à l'article 24.1 de la Charte. On a vu une telle situation survenir à l'occasion de la constitution des banques de données servant à alimenter les logiciels de reconnaissance faciale, par exemple[284]. Ainsi, d'après les auteures d'une étude du Citizen Lab de l'Université de Toronto, les technologies algorithmiques de maintien de l'ordre menacent le droit inscrit à 24.1 de façon nouvelle et significative[285]. Par exemple, les informations peuvent ne pas être sujettes aux mêmes cadres juridiques que d'autres données collectées par les gouvernements[286].

En outre, les systèmes de décision automatisée sont susceptibles d'avoir un impact sur les intérêts protégés par l'article 24.1 de la Charte, entre autres parce qu'elles doivent, de façon inhérente, recueillir des masses de données aussi bien aux fins d'entraînement qu'aux fins d'analyse[287].

Le Haut-Commissariat des Nations Unies aux droits de l'homme s'est aussi prononcé sur la question :

> Les agrégations d'informations communément appelées «métadonnées» peuvent donner des indications sur la conduite d'un individu, ses relations sociales, ses préférences privées et son identité qui vont bien au-delà de ce que l'on obtient en accédant au contenu d'une communication privée.[288]
>
> Il s'ensuit que tout captage de données sur les communications constitue potentiellement une immixtion dans la vie privée et qu'en outre, la collecte et la conservation de ces données constituent également une telle ingérence, que les données soient ou non consultées ou utilisées par la suite. La possibilité qu'une information relative à des communications soit interceptée constitue même à elle seule une immixtion dans la vie privée et peut être attentatoire à des droits, y compris ceux relatifs à la liberté d'expression et d'association. Ainsi, l'existence même d'un programme de surveillance de masse constitue une immixtion dans la vie privée. Il reviendra à l'État de démontrer que cette immixtion n'est ni arbitraire ni illégale.[289]

---

284 Voir notamment *infra*, section 1.2.

285 K. ROBERTSON, C. KHOO et Y SONG, préc., note 22, p. 74.

286 *Id.*

287 Petre MOLNAR et Lex GILL, *Bots at the Gates – A human rights analysis of automated decision-making in Canada's immigration and refugee system*, Citizen Lab et International Human Rights Program (Faculty of Law, University of Toronto), 2018. p. 42.

288 *Le droit à la vie privée à l'ère du numérique*, préc., note 21, par. 19.

289 *Id.*, par. 20.

Le chapitre de la Charte portant sur les droits judiciaires comporte également le droit à une audition publique et impartiale :

> « 23. Toute personne a droit, en pleine égalité, à une audition publique et impartiale de sa cause par un tribunal indépendant et qui ne soit pas préjugé, qu'il s'agisse de la détermination de ses droits et obligations ou du bien-fondé de toute accusation portée contre elle.
>
> Le tribunal peut toutefois ordonner le huis clos dans l'intérêt de la morale ou de l'ordre public. »[290]

Le tribunal dont il est question dans l'article 23 inclut un coroner, un commissaire-enquêteur sur les incendies, une commission d'enquête ou une personne ou un organisme exerçant des fonctions quasi judiciaires[291].

La Cour supérieure a reconnu le rapport qui existe entre l'article 23 de la Charte et l'adage « nul ne peut se faire justice lui-même », « puisque celui qui se fait justice lui-même prive ainsi la victime de son droit d'être entendu par un tribunal »[292]. L'interdiction de se faire justice soi-même tire sa source de la primauté du droit[293]. Ce principe s'appliquerait aussi bien aux institutions publiques que privées[294], « quels que soient les reproches que l'on peut avoir contre une personne »[295].

Le principe est confirmé par l'article 24 de la Charte qui indique :

> 24. Nul ne peut être privé de sa liberté ou de ses droits, sauf pour les motifs prévus par la loi et suivant la procédure prescrite.

---

290 Charte, art. 23 (notre soulignement).

291 *Id.,* art. 56.

292 *Ghaho* c. *Germain*, 2013 QCCS 2604, par. 65.

293 *Conseil de l'éducation de Toronto (Cité)* c. *F.E.E.E.S.O., district 15*, [1997] 1 R.C.S. 487, par. 95.

294 René DUSSAULT et Louis BORGEAT, *Traité de droit administratif*, 2e éd., tome 1, Québec, Presses de l'Université Laval, 1984, p. 357.

295 *Lapierre* c. *Pelletier*, 1994 CanLII 3589 (QC C.A.), par. 20.

La jurisprudence de la Cour du Québec conclut que l'interdiction faite par l'article 24 s'applique à des acteurs privés[296].

Comme la Commission le notait récemment à l'égard des dossiers de crédit[297] et en ce qui concerne le recours à des systèmes d'intelligence artificielle[298], les droits judiciaires pourraient être compromis par le recours à des processus automatisés de prises de décision qui ne seraient pas suffisamment accessibles et transparents et qui ne permettraient pas à la personne concernée d'être entendue et de contester la décision qui est prise à son égard. Nous y reviendrons.

2.2.6 Le droit de vivre dans un environnement sain et respectueux de la biodiversité

Les discussions qui entourent la collecte et l'utilisation des renseignements personnels donnent souvent une impression d'immatérialité. On pense par exemple à l'expression « infonuagique » qui laisse entendre que nos données flottent légèrement dans le ciel[299]. Or, en réalité, les centres de stockages occupent des espaces de plus en plus importants. Ils ne sont pas non plus sans impact environnemental.

Les centres de stockage de données nécessitent des quantités importantes d'eau et d'énergie pour fonctionner et génèrent des déchets néfastes pour l'environnement[300]. Selon des experts, l'empreinte carbone des centres de stockage grandit plus rapidement que celle de tout autre domaine technologique[301]. Qui plus est, comme mentionné plus haut, la croissance des entreprises qui sont au centre de ces développements technologiques dépend d'une génération et d'un stockage toujours plus grands de données. On peut donc supposer que l'espace occupé

---

296 *Chevrier* c. *VCS investigation inc*., 2000 CanLII 14703 (QC C. Q.); *Kupriakov* c. *Gestion René J. Beaudoin inc. (Canadian Tire)*, 2012 QCCQ 5778. Ces décisions ont été rendues en matière de privation de liberté. On peut présumer que l'article 24 s'applique également aux acteurs privés quand ceux-ci privent une personne de ses droits.

297 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 11, p. 25 et suivantes (section 3).

298 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 13, p. 15 et suivantes.

299 Federica LUCIVERO, « Big Data, Big Waste? A Reflection on the Environmental Sustainability of Big Data Initiatives », (2020) 26-2 *Sci Eng Ethics* 1009, 1018.

300 *Id*., p. 1014-1015.

301 *Id*., p. 1015.

par les centres de stockage ainsi que leurs impacts environnementaux sont appelés à croître[302]. Il convient d'en tenir compte puisque la Charte garantit, à son article 46.1 le « droit de vivre dans un environnement sain et respectueux de la biodiversité. »

3 L'ANALYSE DU PROJET DE LOI EN REGARD DES DROITS ET LIBERTÉS EN CAUSE

3.1 Le traitement des données

Le traitement des données soulève d'importants enjeux quant à la protection des droits et libertés de la personne. Le professeur Déziel indique :

> [L] a protection efficace du droit à la vie privée exige aujourd'hui une définition plus précise des fins du traitement de l'information qui peuvent être qualifiées d'acceptables et de raisonnables au sens de la loi, de même qu'une identification plus claire du type de renseignements qui peuvent faire l'objet d'une collecte dans la poursuite de ces objectifs.[303]

Le projet de loi nº 64 tente à quelques reprises de mieux encadrer les fins auxquelles les renseignements personnels sont recueillis.

Par exemple, il introduirait à la Loi sur le public une obligation d'informer les personnes physiques en cas de recours à certaines technologies :

> 65.0.1. En plus des informations devant être fournies suivant l'article 65, quiconque recueille des renseignements personnels auprès de la personne concernée en ayant recours à une technologie comprenant des fonctions permettant de l'identifier, de la localiser ou d'effectuer un profilage de celle-ci doit, au préalable, l'informer:
>
> 1° du recours à une telle technologie;
>
> 2° des moyens offerts, le cas échéant, pour désactiver les fonctions permettant d'identifier, de localiser ou d'effectuer un profilage.

---

302 *Id*., p. 1016.

303 Pierre-Luc DÉZIEL, « Est-ce bien nécessaire? Le principe de limitation de la collecte face aux défis de l'intelligence artificielle et des données massives » dans SERVICE DE LA QUALITÉ DE LA PROFESSION, BARREAU DU QUÉBEC, *Développements récents en droit à la vie privée*, Vol. 465, 2019, 1, p. 24 [En ligne]. https://edoctrine.caij.qc.ca/developpements-recents/465/369051329/

> Le profilage s'entend de la collecte et de l'utilisation de renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement de cette personne.[304]

Une disposition identique serait incluse à la Loi sur le privé[305].

Le projet de loi introduirait également la notion de traitement automatisé des données à la Loi sur le public ainsi qu'à la Loi sur le privé. En effet, il ajouterait l'article suivant à la Loi sur le public :

> 65.2. Un organisme public qui utilise des renseignements personnels afin que soit rendue une décision fondée exclusivement sur un traitement automatisé de ceux-ci doit, au moment de la décision ou avant, en informer la personne concernée.
>
> Il doit aussi, à la demande de la personne concernée, l'informer :
>
> 1° des renseignements personnels utilisés pour rendre la décision;
>
> 2° des raisons, ainsi que des principaux facteurs et paramètres, ayant mené à la décision;
>
> 3° de son droit de faire rectifier les renseignements personnels utilisés pour rendre la décision.[306]

Dans le même esprit, il introduirait la disposition suivante à la Loi sur le privé :

> 12.1. Toute personne qui exploite une entreprise et qui utilise des renseignements personnels afin que soit rendue une décision fondée exclusivement sur un traitement automatisé de ceux-ci doit, au moment de la décision ou avant, en informer la personne concernée.
>
> Elle doit aussi, à la demande de la personne concernée, l'informer :
>
> 1° des renseignements personnels utilisés pour rendre la décision;
>
> 2° des raisons, ainsi que des principaux facteurs et paramètres, ayant mené à la décision;
>
> 3° de son droit de faire rectifier les renseignements personnels utilisés pour rendre la décision.

304 Projet de loi nº 64, art. 18.

305 *Id.*, art. 99 qui introduirait l'art. 8.1 à Loi sur le privé.

306 *Id.*, art. 20.

> Il doit être donné à la personne concernée l'occasion de présenter ses observations à un membre du personnel de l'entreprise en mesure de réviser la décision.[307]

Enfin il modifierait l'article 65.1 de la Loi sur le public en vue de permettre un usage différent des fins pour lequel il a été recueilli dans certaines circonstances. Le nouvel article se lirait comme suit :

> 65.1. ~~Un renseignement personnel ne peut être utilisé au sein d'un organisme public qu'aux fins pour lesquelles il a été recueilli.~~
>
> Un renseignement personnel ne peut être utilisé au sein d'un organisme public qu'aux fins pour lesquelles il a été recueilli, à moins du consentement de la personne concernée. Ce consentement doit être manifesté de façon expresse dès qu'il s'agit d'un renseignement personnel sensible.
>
> ~~L'organisme public peut toutefois utiliser un tel renseignement à une autre fin avec le consentement de la personne concernée ou, sans son consentement, dans les seuls cas suivants:~~
>
> ~~1° lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli;~~
>
> ~~2° lorsque son utilisation est manifestement au bénéfice de la personne concernée;~~
>
> ~~3° lorsque son utilisation est nécessaire à l'application d'une loi au Québec, que cette utilisation soit ou non prévue expressément par la loi.~~
>
> L'organisme public peut toutefois utiliser un renseignement personnel à une autre fin sans le consentement de la personne concernée dans les seuls cas suivants:
>
> 1° lorsque son utilisation est à des fins compatibles avec celles auxquelles il a été recueilli;
>
> 2° lorsque son utilisation est manifestement au bénéfice de la personne concernée;
>
> 3° lorsque son utilisation est nécessaire à l'application d'une loi au Québec, que cette utilisation soit ou non prévue expressément par la loi;
>
> 4° lorsque son utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé.
>
> Pour qu'une fin soit compatible au sens du paragraphe 1° du deuxième alinéa, il doit y avoir un lien pertinent et direct avec les fins pour lesquelles le renseignement a été recueilli.
>
> Lorsqu'un renseignement est utilisé dans l'un des cas visés aux paragraphes 1° à 3° du deuxième alinéa, le responsable de la protection des renseignements personnels au sein de l'organisme doit inscrire l'utilisation dans le registre prévu à l'article 67.3.

307 *Id.*, art. 102.

> Pour l'application de la présente loi, un renseignement personnel est dépersonnalisé lorsque ce renseignement ne permet plus d'identifier directement la personne concernée.[308]

On retrouverait à la Loi sur le privé une disposition similaire :

> 12. Un renseignement personnel ne peut être utilisé au sein de l'entreprise qu'aux fins pour lesquelles il a été recueilli, à moins du consentement de la personne concernée. Ce consentement doit être manifesté de façon expresse dès qu'il s'agit d'un renseignement personnel sensible.
>
> Un renseignement personnel peut toutefois être utilisé à une autre fin sans le consentement de la personne concernée dans les seuls cas suivants :
>
> 1° lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli;
>
> 2° lorsque son utilisation est manifestement au bénéfice de la personne concernée;
>
> 3° lorsque son utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé.
>
> Pour qu'une fin soit compatible au sens du paragraphe 1° du deuxième alinéa, il doit y avoir un lien pertinent et direct avec les fins auxquelles le renseignement a été recueilli. Toutefois, ne peut être considérée comme une fin compatible la prospection commerciale ou philanthropique.
>
> Pour l'application de la présente loi, un renseignement personnel est :
>
> 1° dépersonnalisé lorsque ce renseignement ne permet plus d'identifier directement la personne concernée;
>
> 2° sensible lorsque, de par sa nature ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée.[309]

À notre avis, il s'agit d'un pas vers un élargissement de la portée des règles concernant la protection les renseignements personnels pour inclure, suivant l'expression du professeur Déziel, les fins du traitement qui est fait de ces données.

L'élargissement proposé par le projet de loi nous semble nécessaire pour protéger les autres droits garantis par la Charte. Comme le souligne le professeur de droit Frank Pasquale en ce qui concerne le droit à la sauvegarde de sa réputation, « cela signifierait de focaliser moins, en

---

308 Loi sur le public, art. 65.1 tel qu'il serait modifié par le projet de loi nº 64, art. 19 [les ajouts ont été soulignés et les retranchements, biffés.].

309 Projet de loi n°64, art. 102.

amont, sur la collecte des données et plus sur leur usage – la façon dont les compagnies et les gouvernements les exploitent effectivement pour prendre des décisions »[310]. [Notre traduction.]

Nous sommes d'avis que le commentaire s'applique à tous les autres droits garantis par la Charte et qui sont susceptibles d'être compromis par le traitement des renseignements personnels.

3.1.1 Le traitement automatisé des renseignements personnels

L'élargissement proposé au projet de loi quant au traitement automatisé des renseignements personnels s'apparente au « droit à l'explication » prévu au *Règlement général sur la protection des données*[311] européen. Or, certains expriment des réserves quant à la portée de ce droit dans le contexte européen[312]. Premièrement, le type d'information qui est fourni à la personne n'est pas spécifié :

> Il n'est pas clair s'il s'agit seulement d'un droit à une explication générale du modèle du système dans son ensemble (explication basée sur le modèle) plutôt qu'un droit à une explication à savoir comment une décision a été prise sur la base des faits particuliers d'un sujet de données particulier (explication basée sur le sujet).[313] [Notre traduction.]

Deuxièmement, le droit à l'explication est limité aux décisions basées sur des renseignements personnels, et ce, alors que des décisions automatisées peuvent affecter les droits et libertés des personnes même si leurs renseignements personnels ne sont pas traités ou encore s'ils le sont indirectement sous forme agrégée après avoir été « anonymisés »[314].

---

310 Frank PASQUALE, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge, Harvard University Press, 2019, p. 140-141.

311 *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (règlement général sur la protection des données), JOUE L127 2 du 23 mai 2018, art. 13-15 (ci-après « RGPD »).

312 Voir notamment, Lilian EDWARDS et Michael VEALE, « Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"? », (2018) 16 (3) *IEEE Security & Privacy* 46; Frederick J. ZUIDERVEEN BORGESIUS, « Strenghtening legal protection against discrimination by algorithms and artificial intelligence », *The International Journal of Human Rights*, 2020, DOI: 10.1080/13642987.2020.1743976, p. 9-11, [En ligne]. https://www.tandfonline.com/doi/full/10.1080/13642987.2020.1743976

313 L. EDWARDS et M. VEALE, *id.*, p. 48.

314 *Id.*

À ce sujet, dans son mémoire sur les systèmes d'intelligence artificielle, la Commission a affirmé qu'un « renseignement inféré devrait être considéré comme un renseignement personnel au même titre qu'un renseignement colligé »[315]. Troisièmement, le droit à l'explication place le fardeau de la contestation d'une décision automatisée sur la personne qui y est soumise. Certains s'inquiètent donc que le droit à l'explication puisse constituer une « transparency fallacy »[316].

Le professeur de droit Frederick J. Zuiderveen Borgesius identifie plusieurs limites au potentiel de protection contre la discrimination algorithmique des lois de protection des renseignements[317]. Premièrement, il existe un déficit de conformité et de mise en application et les « autorités de contrôle »[318] sont surchargées. Deuxièmement, comme mentionné, les décisions automatisées aux effets discriminatoires ne concernent pas seulement les renseignements personnels au sens strict :

> Puisque la législation sur la protection des données s'applique seulement aux données personnelles, les processus décisionnels algorithmiques sont partiellement à l'extérieur de son champ d'application. La législation sur la protection des données ne s'applique pas aux modèles prédictifs puisqu'ils ne se rapportent pas à des personnes identifiables. Par exemple, un modèle prédictif qui dit que 80 % des gens résidant dans le code postal 10017 paient leurs factures en retard. Ainsi, le modèle n'est pas une donnée personnelle. (La législation sur la protection des données s'applique quand un tel modèle prédictif est appliqué à un individu).[319] [Notre traduction.]

Troisièmement, les règlements sur les renseignements sensibles peuvent faire en sorte que des organisations ne collectent pas de telles données, ce qui complique l'identification de pratiques de discrimination par proxy[320]. Enfin, en dépit du droit à l'explication, il est pratiquement impossible d'expliquer le processus décisionnel étant donné la quantité de données traitées.

---

315 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 13, p. 13.

316 L. EDWARDS et M. VEALE, préc., note 312, p. 48.

317 F. J. ZUIDERVEEN BORGESIUS, préc., note 312, p. 10.

318 En vertu de l'article 51 du RGPD, les États membres doivent instituer une ou plusieurs autorités de contrôle, soit des autorités publiques indépendantes responsables de la surveillance de l'application du règlement.

319 F. J. ZUIDERVEEN BORGESIUS, préc., note 312, p. 10.

320 Voir notamment Monique MANN et Tobias MATZNER, « Challenging algorithmic profiling : The limits of data protection and anti-discrimination in responding to emergent discrimination », (2019) 6:2 *Big Data & Society*, [En ligne]. https://journals.sagepub.com/doi/pdf/10.1177/2053951719895805; Michael VEALE et Reuben BINNS, « Fairer machine learning in the real world: Mitigating Discrimination without collecting sensitive

Suivant ce qui a été observé en Europe, si l'élargissement proposé par le projet de loi en matière d'information quant aux décisions automatisées est nécessaire, il ne nous apparaît cependant pas suffisant.

L'utilisation des renseignements personnels aux fins de prise de décision automatisée ne conférerait que le droit d'être informé de ce traitement et de rectifier les renseignements qui seraient utilisés, et ce, seulement si la décision est fondée exclusivement sur le traitement automatisé. Il ne prévoit pas la transparence du processus de traitement ou la possibilité de contester le résultat produit et il ne confère absolument aucun droit si la décision n'est pas fondée exclusivement sur un traitement automatisé. Or, les organismes publics ont aussi recours à des logiciels de traitement automatisé des données pour les aider dans leur prise de décision, ce qui affecte les droits des administrés[321]. Le projet de loi ne prévoit pas non plus de définition des notions de « traitement » ou de « traitement automatisé ».

RECOMMANDATION 1

> **La Commission recommande de retirer le terme « exclusivement » de l'article 65.2 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* tel qu'il serait modifié par l'article 20 du projet de loi nº 64 et de l'article 12.1 de la *Loi sur la protection des renseignements personnels dans le secteur privé* tel qu'il serait introduit par l'article 102 du projet de loi nº 64.**

RECOMMANDATION 2

> **La Commission recommande que le projet de loi nº 64 prévoie que l'utilisation des renseignements personnels aux fins de prise de décision automatisée confère le droit à une intervention humaine ainsi que le droit de contester le résultat ainsi produit.**

Pour sa part, le droit d'être informé du recours à une technologie comprenant des fonctions permettant d'identifier, de localiser ou d'effectuer le profilage d'une personne qui serait introduit

---

data », (2017) 4:2 *Big Data & Society*, [En ligne]. https://journals.sagepub.com/doi/full/10.1177/2053951717743530

321 C'est notamment le cas dans en matière d'immigration et de détermination du statut de réfugié. Voir P. MOLNAR et L. GILL, préc., note 287

à la Loi sur le public[322] et à la Loi sur le privé[323] ne donne pas le droit de s'opposer à un tel recours. En outre, il ne prévoit pas d'obligation de prévoir des mécanismes pour désactiver ces fonctions.

Pourtant, comme la Commission l'a déjà indiqué[324], le traitement automatisé des renseignements personnels - notamment par le recours à l'intelligence artificielle - est susceptible de compromettre plusieurs des droits garantis par la Charte, notamment la liberté de sa personne[325] et les libertés fondamentales[326], le droit à la sauvegarde de sa dignité, de son honneur et de sa réputation[327], le droit au respect de sa vie privée[328], le droit à la reconnaissance et à l'exercice, en pleine égalité, des droits et libertés[329], le droit à une audition publique et impartiale de sa cause par un tribunal indépendant et qui ne soit pas préjugé[330] ainsi que le droit de ne pas être privé de sa liberté ou de ses droits sauf pour les motifs prévus par la loi[331].

Par contraste, en Europe, le RGPD énonce, dans son préambule :

> Les principes et les règles régissant la protection des personnes physiques à l'égard du traitement des données à caractère personnel les concernant devraient, quelle que soit la nationalité ou la résidence de ces personnes physiques, respecter leurs libertés et droits fondamentaux, en particulier leur droit à la protection des données à caractère personnel.[332]

---

322 Projet de loi nº 64, art. 18.

323 *Id.*, art. 99.

324 Voir, *infra*, section 2; Voir également COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 13; COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 14.

325 Charte, art. 1er.

326 *Id.*, art. 3.

327 *Id.*, art. 4.

328 *Id.*, art. 5.

329 *Id.*, art. 10

330 *Id.*, art. 23.

331 *Id.*, art. 24.

332 RGPD, 2e considérant du Préambule.

Ce règlement prévoit également que le traitement des données doit être licite et explicite ce en quoi consiste la licéité[333].

L'article 22 du RGPD prohibe en outre certaines décisions fondées sur le traitement automatisé des données :

> Article 22
>
> Décision individuelle automatisée, y compris le profilage
>
> La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.
>
> Le paragraphe 1 ne s'applique pas lorsque la décision:
>
> est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement;
>
> est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée; ou
>
> est fondée sur le consentement explicite de la personne concernée. […][334]

En ce qui a trait aux « effets juridiques » ou « l'affectant de manière significative de façon similaire », Zuiderveen Borgesius donne les exemples suivants :

> Qu'est-ce qu'une décision produisant des « effets juridiques »? Un exemple est une décision d'un tribunal ou une décision concernant une prestation sociale octroyée par la loi, comme des paiements de retraite. Un exemple de décision « affectant de manière significative » est une décision prise par une banque pour refuser le crédit à quelqu'un.[335] [Renvoi omis, notre traduction.]

Le champ d'application de l'article 22 du RGPD n'inclut cependant pas des décisions automatisées telles de la publicité ciblée ou la dissémination de fausses nouvelles qui, de façon agrégée, ont pourtant des effets significatifs sur la société[336].

---

333 *Id.*, art. 6; La notion de « traitement » est définie à l'art. 4 du RGPD.

334 *Id.*, art. 22, par. 1.

335 F. J. ZUIDERVEEN BORGESIUS, préc., note 312, p. 8.

336 L. EDWARDS et M. VEALE, préc., note 312.

Même si l'on peut penser que les utilisateurs ne lisent pas les notices relatives à la vie privée fournissant de l'information sur l'utilisation des renseignements personnels dans les décisions automatisées, des chercheurs, des journalistes et des autorités de contrôle sont en mesure de mieux s'informer sur les pratiques des organisations[337]. L'obligation de transparence en la matière est donc susceptible de contribuer à réduire les risques de violations des droits et libertés de la personne, notamment de discrimination. Ces protections sont nécessaires dans la mesure où les systèmes algorithmiques sont caractérisés par le problème dit de la « boîte noire », c'est-à-dire que leurs fonctionnements internes sont opaques. En raison de cette opacité, il est difficile pour une personne de savoir qu'elle est victime de discrimination et, le cas échéant, d'en faire la démonstration[338].

En vertu du RGPD, lorsqu'une pratique comporte des risques importants d'atteintes aux droits et libertés, les organisations sont également tenues de mener une analyse d'impact relative à la protection des données, incluant les risques de discrimination[339] :

> Article 35
>
> Analyse d'impact relative à la protection des données
>
> Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

Le RGPD accorde également le droit d'obtenir une intervention humaine de la part du responsable du traitement ainsi que le droit à l'expression du point et à la contestation de la décision[340].

337 F. J. ZUIDERVEEN BORGESIUS, préc., note 312 , p. 9.

338 *Id.* p. 6.

339 *Id.* p. 8.

340 RGPD, art. 22, par 3.

RECOMMANDATION 3

La Commission recommande que les articles 18 et 64 du projet de loi nº 64 soient modifiés afin de prévoir que le recours à une technologie permettant d'identifier, de localiser ou d'effectuer le profilage d'une personne confère le droit de s'opposer à un tel recours et oblige à prévoir des mécanismes pour désactiver ces fonctions.

RECOMMANDATION 4

La Commission recommande que le projet de loi nº 64 soit modifié afin de prévoir un droit à l'explication pour l'ensemble des décisions qui prennent appui sur un traitement automatisé des renseignements personnels.

3.1.2 L'utilisation des renseignements personnels à des fins compatibles sans le consentement de la personne concernée

Comme mentionné plus haut, le projet de loi propose d'introduire dans la Loi sur le privé la possibilité pour une entreprise d'utiliser un renseignement personnel « à une autre fin sans le consentement de la personne concernée » lorsque « son utilisation est à des fins compatibles avec celles auxquelles il a été recueilli »[341]. Une fin sera considérée comme compatible lorsqu'il existe « un lien pertinent et direct avec les fins pour lesquelles le renseignement a été recueilli[342]. » De plus, ne pourra être considérée comme compatible « la prospection commerciale ou philanthropique »[343].

L'article proposé est calqué sur l'article 65.1 de la Loi sur public, qui a été introduit en 2006 par le projet de loi nº 86[344]. Dans son mémoire sur ce projet de loi, la Commission s'était opposée à cette exception à l'exigence d'obtenir le consentement, considérant qu'il s'agit d'une « une entorse majeure aux principes régissant la protection des renseignements personnels dans la Loi sur l'accès. »[345] La Commission soulignait aussi l'absence de mesures de contrôle ou

341 Projet de loi nº 64, art. 102.

342 Loi sur le public art. 65.1 et projet de loi nº 64, art. 102.

343 Projet de loi nº 64, art. 102.

344 *Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives*, projet de loi nº 86 (sanction – 14 juin 2006) 1re sess. 37e leg. (Qc).

345 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Mémoire à la Commission de la culture de l'Assemblée nationale sur le Projet de loi 86, Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives*, (Cat. 2.412.42.5), 2005, p. 16.

d'obligation d'informer la CAI de telles utilisations. Comme elle l'affirmait, il s'agit d'une « brèche importante dans le principe de finalité »[346], nécessaire à l'obtention d'un consentement valide. Ces observations demeurent pertinentes tant pour l'article existant de la Loi sur le public que pour la disposition proposée pour la Loi sur le privé. La Commission réitère donc sa recommandation, avec les adaptations nécessaires :

RECOMMANDATION 5

La Commission recommande que les seuls cas où un organisme public ou une entreprise puisse utiliser un renseignement personnel à d'autres fins que celles pour lesquelles il ou elle l'a recueilli soient :

- **avec le consentement de la personne concernée;**
- **si l'utilisation est nécessaire à l'application d'une loi au Québec, après en avoir informé la Commission d'accès à l'information; ou**
- **sur autorisation de la Commission d'accès à l'information.**

À tout le moins, il nous semble nécessaire de mieux circonscrire ce qui peut être qualifié de « fins compatibles » afin de limiter les atteintes aux droits qui pourraient résulter de cette utilisation. Le préambule du RGPD précise quant à lui que :

> Afin d'établir si les finalités d'un traitement ultérieur sont compatibles avec celles pour lesquelles les données à caractère personnel ont été collectées initialement, le responsable du traitement, après avoir respecté toutes les exigences liées à la licéité du traitement initial, devrait tenir compte, entre autres: de tout lien entre ces finalités et les finalités du traitement ultérieur prévu; du contexte dans lequel les données à caractère personnel ont été collectées, en particulier les attentes raisonnables des personnes concernées, en fonction de leur relation avec le responsable du traitement, quant à l'utilisation ultérieure desdites données; la nature des données à caractère personnel; les conséquences pour les personnes concernées du traitement ultérieur prévu; et l'existence de garanties appropriées à la fois dans le cadre du traitement initial et du traitement ultérieur prévu.[347]

Nous recommandons donc de préciser la notion de fins compatibles.

RECOMMANDATION 6

La Commission recommande, le cas échéant, de préciser et circonscrire la notion de fins compatibles dans le respect des droits et libertés de la personne garantis par la Charte, notamment en ce qui a trait au droit au respect de sa vie privée.

---

346 *Id*.

347 RGPD, 50e considérant du Préambule.

Finalement, la Commission est particulièrement inquiète de la possibilité d'utiliser des renseignements sensibles à des fins compatibles sans le consentement de la personne concernée. Nous reviendrons sur l'importance de protéger adéquatement ces renseignements plus bas. De notre avis, si la recommandation 5 n'est pas suivie, cette exception relative au consentement ne devrait pas s'appliquer aux renseignements personnels sensibles.

RECOMMANDATION 7

> **La Commission recommande, le cas échéant, que les renseignements personnels sensibles ne puissent être utilisés à des fins compatibles sans le consentement de la personne concernée.**

3.2 La notion de « renseignement personnel sensible »

Le projet de loi nº 64 introduirait la notion de renseignement personnel sensible à la Loi sur le public et à la Loi sur le privé. L'article 59 de la Loi sur le public serait modifié de la façon suivante :

> Un organisme public ne peut communiquer un renseignement personnel sans le consentement de la personne concernée. Ce consentement doit être manifesté de façon expresse dès qu'il s'agit d'un renseignement personnel sensible.
>
> Toutefois, il peut communiquer un ~~tel renseignement sans le consentement de cette personne~~ renseignement personnel sans le consentement de la personne concernée, dans les cas et aux strictes conditions qui suivent :
>
> 1° au procureur de cet organisme si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi que cet organisme est chargé d'appliquer, ou au Directeur des poursuites criminelles et pénales si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi applicable au Québec;
>
> 2° au procureur de cet organisme, ou au procureur général lorsqu'il agit comme procureur de cet organisme, si le renseignement est nécessaire aux fins d'une procédure judiciaire autre qu'une procédure visée dans le paragraphe 1°;
>
> 3° à une personne ou à un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois, si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi applicable au Québec;
>
> 4° à une personne à qui cette communication doit être faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée;
>
> ~~5° à une personne qui est autorisée par la Commission d'accès à l'information, conformément à l'article 125, à utiliser ce renseignement à des fins d'étude, de recherche ou de statistique;~~
>
> 6° (paragraphe abrogé);
>
> 7° (paragraphe abrogé);

8° à une personne ou à un organisme, conformément aux articles ~~61, 66, 67, 67.1, 67.2, 68 et 68.1~~ 61, 63.7, 66, 67, 67.1, 67.2, 67.2.1, 68 et 70.5;

9° à une personne impliquée dans un événement ayant fait l'objet d'un rapport par un corps de police ou par une personne ou un organisme agissant en application d'une loi qui exige un rapport de même nature, lorsqu'il s'agit d'un renseignement sur l'identité de toute autre personne qui a été impliquée dans cet événement, sauf s'il s'agit d'un témoin, d'un dénonciateur ou d'une personne dont la santé ou la sécurité serait susceptible d'être mise en péril par la communication d'un tel renseignement.

Pour l'application de la présente loi, un renseignement personnel est sensible lorsque, de par sa nature ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée.[348]

Le projet de loi nº 64 prévoit le remplacement des articles 12 et 13 de la Loi sur le privé par les suivants :

12. Un renseignement personnel ne peut être utilisé au sein de l'entreprise qu'aux fins pour lesquelles il a été recueilli, à moins du consentement de la personne concernée. Ce consentement doit être manifesté de façon expresse dès qu'il s'agit d'un renseignement personnel sensible.

Un renseignement personnel peut toutefois être utilisé à une autre fin sans le consentement de la personne concernée dans les seuls cas suivants :

1° lorsque son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli;

2° lorsque son utilisation est manifestement au bénéfice de la personne concernée;

3° lorsque son utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé.

Pour qu'une fin soit compatible au sens du paragraphe 1° du deuxième alinéa, il doit y avoir un lien pertinent et direct avec les fins auxquelles le renseignement a été recueilli. Toutefois, ne peut être considérée comme une fin compatible la prospection commerciale ou philanthropique.

Pour l'application de la présente loi, un renseignement personnel est :

1° dépersonnalisé lorsque ce renseignement ne permet plus d'identifier directement la personne concernée;

2° sensible lorsque, de par sa nature ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée.

[…]

13. Nul ne peut communiquer à un tiers les renseignements personnels qu'il détient sur autrui, à moins que la personne concernée n'y consente ou que la présente loi ne le prévoie.

348 Loi sur le public, art. 59 tel qu'il serait modifié par l'article 12 du projet de loi nº 64. Les ajouts sont surlignés et les parties qui seraient abrogées sont biffées.

> Le consentement doit être manifesté de façon expresse dès qu'il s'agit d'un renseignement personnel sensible.

Le projet de loi prévoit donc la même définition de la notion de renseignement sensible dans la cadre de la Loi sur le public que dans le cadre de la Loi sur le privé, soit un renseignement qui « de par sa nature ou en raison du contexte de son utilisation, […] suscite un haut degré d'attente raisonnable en matière de vie privée »[349].

Nous sommes d'avis que le législateur ne devrait pas recourir à l'expression « attente raisonnable de vie privée ». Autrement, cela perpétuerait la confusion qui existe entre, d'une part, la notion de vie privée qui découle de l'interdiction des fouilles, des saisies et des perquisitions abusives qui existe en vertu des dispositions de la Charte canadienne et de la Charte québécoise et, d'autre part, le droit au respect de sa vie privée qui est garanti par la Charte québécoise. À notre avis, le recours à une telle notion pose une limite au droit au respect de sa vie privée, soit l'attente raisonnable de vie privée, qui n'existe pas à l'égard du droit au respect de sa vie privée tel que le consacre la Charte québécoise.

RECOMMANDATION 8

> **La Commission recommande que la notion « d'attente raisonnable de vie privée » soit retirée du projet de loi nº 64.**

Par ailleurs, la Commission a par le passé fait part de préoccupations en ce qui concerne la sensibilité des informations de santé, des renseignements génétiques, les dossiers de crédit et les informations contenues dans les dossiers de police, notamment.

3.2.1 Les informations de santé

De l'avis de la Commission, les informations de santé sont « hautement sensibles »[350]. La Commission s'est également prononcée sur la convoitise spécifique à l'égard de ces

---

349 Voir *infra*, section 2.1.2.

350 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Mémoire à la Commission des affaires sociales sur l'avant-projet de loi sur la Carte santé du Québec*, (Cat. 2.412.96), 2002, p. 3 [En lgine]. https://cdpdj.qc.ca/storage/app/media/publications/carte_sante.pdf

informations[351]. Elle reconnaissait alors que plusieurs droits peuvent être affectés lorsqu'il est question de ce type de données :

> Le caractère sensible des données de santé n'est plus à démontrer. Pas plus d'ailleurs que la nécessité de traiter cette information dans le respect du droit au secret professionnel et du droit à la protection des renseignements personnels. Un bris de la confidentialité des renseignements de santé peut également porter atteinte au respect de la réputation d'une personne, à sa vie privée ou encore favoriser la discrimination fondée sur son état de santé.[352]

En 2019, le Commissaire à l'information et à la protection de la vie privée de l'Ontario a ouvert une enquête après que le Toronto Star ait révélé que des données de santé « anonymisées » de millions d'Ontariens ont été vendues à un géant états-unien des données de santé par une entreprise qui vend et gère des logiciels de dossiers médicaux électroniques[353]. Ces données seraient ensuite achetées par des entreprises pharmaceutiques pour élaborer de nouvelles stratégies de mise en marché. Cela serait fait avec le consentement du médecin ou de la clinique, mais sans celui des patients puisque les données sont dites anonymisées et ne correspondraient donc plus formellement à des renseignements personnels.

De plus, alors que les banques de données de santé doivent d'abord être anonymisées ou pseudonymisées avant de pouvoir être utilisées dans le cadre de recherches scientifiques, de récents travaux montrent qu'il est possible de procéder à la réidentification des personnes et que l'anonymisation est donc difficile à concevoir[354]. Les auteurs d'une étude notent ainsi:

---

351 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note10.

352 *Id.* p. 7, citant avec approbation COMMISSION D'ACCÈS À L'INFORMATION, *Avis de la Commission d'accès à l'information concernant l'avant-projet de loi sur la carte santé au Québec*, 8 février 2002, p. 6.

353 Sheryl SPITHOFF, « Privacy Commissioner to investigate sale of health data », *Toronto Star*, 21 février 2019, [En ligne]. https://www.thestar.com/news/investigations/2019/02/21/privacy-commissioner-to-investigate-sale-of-health-data.html ; Sheryl SPITHOFF, « Medical-record software companies are selling your health data », *Toronto Star*, 20 février 2010, [En ligne]. https://www.thestar.com/news/investigations/2019/02/20/medical-record-software-companies-are-selling-your-health-data.html

354 Voir notamment EUROPEAN COMMISSION, WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA (ARTICLE 29 DATA PROTECTION WORKING PARTY), *Opinion 05/2014 on Anonymisation Techniques*, 10 avril 2014, 0829/14/EN WP216, [En ligne]. https://www.pdpjournals.com/docs/88197.pdf; UNESCO, *Steering AI and advanced ICTs for Knowledge societies – A rights, openness, access, and multi-stakeholder perspective*, 2019, p. 49-50, [En ligne]. https://unesdoc.unesco.org/ark:/48223/pf0000372132 ; Luc ROCHER, Julien M. HENDRICKS et Yves-Alexandre DE MONTJOYE, « Estimating the success of re-identifications in incomplete datasets using generative models », *Nature Communications*, 10, 3069, 2019, https://doi.org/10.1038/s41467-019-10933-3, [En ligne]. https://www.nature.com/articles/s41467-019-10933-3#citeas

> Nos résultats suggèrent que, même avec des bases de données anonymisées fortement échantillonnées, il est peu probable de respecter les standards modernes d'anonymisation du RGPD et cela remet sérieusement en doute la suffisante technique et légale du modèle de dépersonnalisation *release-and-forget*[355]. [Notre traduction]

La Commission est donc d'avis que les données de santé dépersonnalisées, comme tous les renseignements personnels dépersonnalisés, doivent continuer à être considérées comme des renseignements personnels[356].

Notons que les données de santé ne sont pas restreintes aux renseignements contenus dans le dossier médical. En effet, comme mentionné plus haut, une foule de données sur la santé des personnes sont générées par des téléphones intelligents ou des appareils intelligents à porter sur soi (*wearables*)[357]. Ces dispositifs peuvent prendre différentes formes et être utilisés, notamment, dans des activités de loisirs, dans le cadre du travail ou dans les dimensions les plus intimes de la vie[358]. Les formes les plus communes sont les montres intelligentes et les moniteurs d'activité physique qui font désormais partie du quotidien de plusieurs. Les applications mobiles et appareils intelligents à porter sur soi peuvent par exemple enregistrer des renseignements nominatifs tels que le nom, l'adresse courriel et le code postal, des données de géolocalisation, des données biométriques comme la taille et le poids et des données sur le rythme cardiaque, le nombre de pas effectués ou la qualité du sommeil qui servent de proxy pour évaluer l'étant de santé physique[359].

---

355 L. ROCHER, J. M. HENDRICKS et Y-A. DE MONTJOYE, *Id.*

356 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 13, p. 24.

357 Voir COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Les appareils intelligents à porter sur soi et la protection de la vie privée », 18 avril 2017, [En Ligne]. https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/appareils-mobiles-et-numeriques/appareils-numeriques/02_05_d_73_wd/ ;

358 Kathryn C. MONTGOMERY, Jeff CHESTER et Katharina KOPP, *Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection*, Center for Digital Democracy, 2016, [En ligne]. https://www.democraticmedia.org/sites/default/files/field/public/2016/aucdd_wearablesreport_final121516.pdf; K. C. MONTGOMERY, J. CHESTER et K. KOPP, préc., note 65; Steven RICHARDSON et Debra MACKINNON, *Left to their own Devices? Privacy Implications of Wearable Technology in Canadian Workplaces*. Surveillance Studies Centre, 2017, [En ligne]. http://www.sscqueens.org/publications/left-to-their-own-devices; I. AJUNWA, K. CRAWFORD et J. SCHULTZ, préc., note 153; Karen E.C. LEVY, « Intimate Surveillance », (2015) *51 Idaho L. Rev.* 679.

359 Nayanika CHALLA, Stephen YU et Sanjay KUNCHAKARRA, « Wary About Wearables: Potential for the Exploitation of Wearable Health Technology Through Employee Discrimination and Sale to Third Parties » (2017) (10:3) *Intersect: The Stanford Journal of Science, Technology, and Society* 2, [En ligne]. http://ojs.stanford.edu/ojs/index.php/intersect/article/view/1003/1065

Il a été révélé des applications mobiles de santé et d'activité physique transmettaient à Facebook des renseignements personnels sensibles comme le rythme cardiaque et le cycle menstruel, et ce, sans le consentement des personnes concernées par ces renseignements[360]. En 2014, une étude de la Federal Trade Commission des États-Unis a révélé que douze applications de santé et d'activité physique avaient transmis des données « sensibles » à 76 tiers, dont des annonceurs publicitaires, et que ces applications n'avaient pas de politiques relatives à la vie privée informant l'utilisateur de la collecte et de la transmission de ses données[361].

Les données produites par ces outils technologiques peuvent notamment être d'intérêt pour un employeur ou susciter la convoitise de compagnies d'assurance ou de l'industrie pharmaceutique[362]. Rappelons que la Commission a déjà fait part de ses inquiétudes quant à l'utilisation des données du dossier de santé par des employeurs ou des assureurs[363]. Elle appelait alors à restreindre l'accès à ces données et à ce « que tout usage de ces informations à des fins autres que celle de la dispensation des soins de santé et de services sociaux puisse faire l'objet d'un débat démocratique et transparent »[364].

De plus, lorsqu'utilisés en milieu de travail, ces appareils intelligents à porter sur soi permettent d'étendre la surveillance au-delà des activités de production pour inclure des données sur la santé et l'ensemble des dimensions de la vie (signes vitaux, émotions, sommeil, alimentation, etc.)[365] Aux États-Unis, dans le cadre de programmes de bien-être, des entreprises ont fourni des montres Fitbit à leurs employés qui pouvaient accumuler des points et les monnayer pour

---

360 Sam SCHECHNER et Mark SECADA, « You Give Apps Sensitive Personal Information. Then They Tell Facebook. », *The Wall Street Journal*, 22 février 2019, [En ligne]. https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636

361 Dans certains cas, cela incluait des données nominatives telles que le nom et l'adresse. Voir N. CHALLA, S. YU et S. KUNCHAKARRA, préc., note 359, 4-5.

362 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 357

363 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 10.

364 *Id.*

365 Voir André SPICER, « Surveillance used to be a bad thing. Now, we happily let our employers spy on us », *The Guardian* (4 août 2017), [En ligne] : https://www.theguardian.com/commentisfree/2017/aug/04/surveillance-employers-spy-implanted-chipped; K. C. MONTGOMERY, J. CHESTER et K. KOPP, préc., note 358, p. 15.

réduire leur prime d'assurances[366]. Cela pose notamment la question du respect de la vie privée et de l'accès aux renseignements personnels :

> Légalement, quand un employeur fournit à un employé un équipement il demeure la propriété de l'employeur, que ce soit un ordinateur portable, un téléphone cellulaire ou un moniteur d'activité physique. Cela signifie que l'employeur peut accéder aux données de cet appareil à tout moment, sans la permission. Ça soulève des questions quant au respect de la vie privée des personnes qui acceptent de participer aux programmes de mieux-être.[367] [Notre traduction.]

De plus, la précision de ces appareils est remise en cause[368] et certains avancent qu'ils seraient particulièrement imprécis pour mesurer le rythme cardiaque des personnes à la peau plus foncée, ce qui pourrait notamment leur porter préjudice dans le cadre de programmes de bien-être imposés par l'employeur, en lien avec des motifs de discrimination interdits, comme la « race », la « couleur » ou l'origine nationale ou ethnique[369].

Les données produites peuvent aussi être monétisées en servant au développement de techniques de marketing ciblées par des entreprises pharmaceutiques dans le but d'influencer le comportement des consommateurs[370].

Selon les chercheur et chercheures Kathryn C. Montgomery, Jeff Chester et Katharina Kopp, bien que les appareils intelligents à porter sur soi qui enregistrent des données de santé peuvent être bénéfiques pour la santé et le bien-être des personnes, notamment pour les personnes avec des problèmes de santé chronique et celles appartenant à des communautés mal desservies par le système de santé, ils sont aussi la source d'inquiétudes en raison des risques de fuites de données, d'utilisation à des fins de marketing manipulateur et de profilage

---

366 Voir Christina FARR, « How Fitbit Became The Next Big Thing In Corporate Wellness », Fast Company (18 avril 2016), [En ligne] : https://www.fastcompany.com/3058462/how-fitbit-became-the-next-big-thing-in-corporate-wellness

367 I. AJUNWA, K. CRAWFORD et J. SCHULTZ, préc., note 153, p. 766-767. Notons que la situation pourrait différer en contexte québécois.

368 Katie SIEK, « Why fitness trackers may not give you all the "credit" you hoped for », *The Conversation*, 15 janvier 2020, [En ligne]. https://theconversation.com/why-fitness-trackers-may-not-give-you-all-the-credit-you-hoped-for-128585

369 Ruth HAILU, « Fitbits and other wearables may not accurately track heart rates in people of color", *Stat*, 24 juillet 2019, [En ligne] : https://www.statnews.com/2019/07/24/fitbit-accuracy-dark-skin/

370 K. C. MONTGOMERY, J. CHESTER et K. KOPP, *Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection*, préc., note 358, p. 5.

discriminatoire par le biais de systèmes de classification algorithmiques qui intégreraient ces données à des informations sur l'ethnicité, l'âge, le genre, la condition médicale, etc.[371]. À leur avis, toutes les données collectées à partir de ces appareils devraient être considérées comme des données sensibles[372]. En ce sens, la protection des renseignements personnels de santé doit être adaptée à l'ère et à l'économie des données massives[373].

3.2.2 Les renseignements génétiques

À l'instar de ce qui est prévu dans le RGPD, les renseignements génétiques devraient de toute évidence être qualifiés de renseignements sensibles. L'utilisation de tels renseignements continue d'être une source importante d'inquiétudes[374]. En plus de relever du droit au respect de la vie privée garanti par la Charte, leur utilisation est susceptible de compromettre l'exercice en pleine égalité des droits et libertés de la personne[375]. Par exemple, leur capacité prédictive présumée peut être la source de discrimination en assurance et en emploi[376].
Comme l'a déjà affirmé la Commission, les renseignements génétiques sont inclus dans le motif de discrimination prohibé « handicap ». En effet, celui-ci reçoit une interprétation large et libérale :

> Les tribunaux interprètent la discrimination fondée sur le handicap comme une « conséquence de perceptions, de mythes ou de stéréotypes ou encore de l'existence de limitations fonctionnelles réelles ». En d'autres termes, un « handicap » peut résulter aussi bien d'une limitation physique que d'une affection, d'une construction sociale, d'une perception de limitation ou d'une combinaison de tous ces facteurs. C'est l'effet de l'ensemble de ces circonstances qui détermine si l'individu est ou non affecté d'un « handicap » pour les fins de la Charte.
>
> L'interprétation du handicap selon la Charte met l'accent sur « les obstacles à la pleine participation plutôt que sur la condition ou l'état de l'individu ».[377]

---

371 *Id.*

372 *Id.*, p. 6.

373 *Id*.

374 *Renvoi relatif à la Loi sur la non-discrimination génétique*, 2020 CSC 17, [En ligne]. https://decisions.scc-csc.ca/scc-csc/scc-csc/fr/18417/1/document.do (consulté le 24 août 2020).

375 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 21, p. 21, COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 94, p. 16 à 18.

376 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 21, p. 21-22.

377 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Rapport de suivi de l'exercice de sensibilisation sur l'accessibilité des commerces au Québec*, Aurélie LEBRUN, (Cat. 2.12-12.60.1), 2015, p. 4,

En vertu des articles 10 et 12 de la Charte, il serait donc interdit de discriminer dans l'offre d'un contrat d'assurance en fonction d'un test génétique. Cependant, la Charte prévoit aussi l'exception suivante :

> Dans un contrat d'assurance ou de rente, un régime d'avantages sociaux, de retraite, de rentes ou d'assurance ou un régime universel de rentes ou d'assurance, une distinction, exclusion ou préférence fondée sur l'âge, le sexe ou l'état civil est réputée non discriminatoire lorsque son utilisation est légitime et que le motif qui la fonde constitue un facteur de détermination de risque, basé sur des données actuarielles.
>
> Dans ces contrats ou régimes, l'utilisation de l'état de santé comme facteur de détermination de risque ne constitue pas une discrimination au sens de l'article 10. [378]

Certains pourraient prétendre que les renseignements génétiques d'une personne font partie de son état de santé et de ce fait justifier la discrimination.

La discrimination fondée sur le handicap est par ailleurs interdite en emploi en vertu de l'article 16 de la Charte. L'employeur dispose cependant d'un moyen de défense quand la distinction, exclusion ou préférence est fondée sur les aptitudes ou qualités requises par un emploi[379]. On peut ainsi penser que les employeurs pourraient être tentés de lier les renseignements génétiques des employés ou futurs employés aux aptitudes ou qualités requises par un emploi en vue de la sélection de candidats, leur maintien en emploi ou leur accès à une promotion[380].

La Commission s'inquiète aussi depuis plusieurs années du fait que :

> [l] es informations génétiques peuvent également comporter une dimension collective, quand on les retrouve agrégées en banques, par exemple aux fins de la génétique des populations. Ainsi, on pourrait craindre des pratiques discriminatoires envers certains

---

[En ligne]. https://www.cdpdj.qc.ca/storage/app/media/publications/rapport_acces_biens_services_Suivi-2015.pdf ; citant *Eaton* c. *Conseil scolaire du Comté de Brant*, [1997] 1 R.C.S. 221, 272 et *Québec (Commission des droits de la personne et des droits de la jeunesse)* c. *Montréal (Ville)*; *Québec (Commission des droits de la personne et des droits de la jeunesse)* c. *Boisbriand (Ville)*, [2000] 1 R.C.S. 665, par. 72 et 82. Voir également : COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Projet de sensibilisation : Vers un accès universel aux biens et services des pharmacies et des établissements d'alimentation (Rapport final)*, Jean-Sébastien Imbeault et M[e] Evelyne Pedneault, (Cat. 2.120.12.60), 2013, p. 10-11, [En ligne]. https://www.cdpdj.qc.ca/storage/app/media/publications/rapport_acces_biens_services.pdf

378 Charte, art. 20.1.

379 *Id.*, art. 20.

380 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 21, p. 25-26.

> groupes en raison des corrélations qui pourraient être faites entre l'origine ethnique et la prévalence de certaines maladies génétiques[381].

La Commission est donc d'avis que la législation québécoise doit offrir une protection suffisante contre toutes les pratiques discriminatoires qui pourraient être liées aux renseignements génétiques.

3.2.3 Les dossiers de crédit

Le dossier de crédit comporte plusieurs informations qui relèvent de la vie privée : nom, adresse, date de naissance, numéro d'assurance sociale, employeur, inventaire des dettes, historique de paiements. La Commission a récemment rappelé les incidences de la constitution du dossier de crédit, l'établissement d'une cote de crédit et la gestion de cette cote sur les droits à la sauvegarde de sa réputation, au respect de sa vie privée et à l'information[382].

L'information concernant le crédit constitue un renseignement personnel, mais, dans l'état du droit actuel, ce n'est pas le cas pour la cote de crédit, ce qui l'exclut des garanties de la Loi sur le privé[383]. La Commision a d'ailleurs recommandé que l'ensemble des cotes de crédit produites par un agent de crédit soient considérées comme des renseignements personnels au sens de la Loi sur le privé afin de garantir aux personnes le droit d'accès aux cotes les concernant et de les faire rectifier[384].

Les droits au respect de sa vie privée, à la sauvegarde de sa réputation et à l'information sont également mis en cause du fait du manque de règles spécifiques encadrant le type

---

381 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *La notion de race dans les sciences et l'imaginaire raciste: la rupture est-elle consommée?*, Daniel Ducharme et Paul Eid, (Cat. 2.500.123), 2006, p. 10-11 [En ligne]. https://cdpdj.qc.ca/storage/app/media/publications/race_science_imaginaire_raciste.pdf ; Ian HACKING, « La race : Pourquoi avons-nous toujours des classifications raciales ? », *Notes de cours de la 6e séance du Cours de philosophie et histoire des concepts scientifiques donnée au Collège de France,* le 22 mars 2005, p. 13-16.

382 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 11, p. 6.

383 *Id.,* p. 13.

384 *Id.*, p. 15.

d'information pouvant être recueillie, la durée durant laquelle les informations peuvent être transmises, l'imputabilité pour la sécurité des données et les usages permis[385].

À cet égard, l'utilisation du dossier de crédit à des fins de sélection des employés, de détermination d'une prime d'assurance, de location de logement ou de marketing peut aller à l'encontre du droit au respect de sa vie privée si les détenteurs des renseignements personnels n'ont pas consenti à ces usages de façon libre, manifeste, éclairée et spécifique[386]. De plus, la Commission a souligné à maintes occasions les effets discriminatoires de l'enquête de crédit, notamment en regard des motifs âge, condition sociale et origine ethnique ou nationale, et ce, dans les domaines du logement et de l'emploi, domaines dans lesquels le « consentement est généralement donné dans un contexte de déséquilibre des parties[387] ». Par exemple, une vérification de crédit au niveau de l'embauche correspond à une question prohibée en vertu des articles 16 et 18.1 de la Charte puisqu'elle implique une collecte discriminatoire d'information sur la condition sociale et, potentiellement, une utilisation discriminatoire de cette information. La Commission a ainsi recommandé que le législateur encadre l'accès et le recours aux dossiers de crédit à des fins autres que celles pour lesquelles ils sont constitués. Le problème de manque de vérification des informations de crédit a aussi été relevé.

3.2.4 Les renseignements contenus dans les dossiers de police

La Commission a régulièrement rappelé son inquiétude face à la communication, dans le cadre de vérifications d'antécédents judiciaires, de renseignements relatifs à des plaintes, des enquêtes ou des arrestations, même quand ces étapes du processus ne mènent pas à une mise en accusation[388], contenus dans les dossiers de police. Ces dossiers peuvent par ailleurs

---

385 *Id.*, p. 17.

386 *Id.*, p. 8-9.

387 *Id.*, p. 24.

388 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *La vérification des antécédents judiciaires des personnes appelées à oeuvrer auprès d'une clientèle vulnérable*, Me Claire BERNARD et Me Pierre BOSSET, (Cat. 2.128.2.5), 1999, p. 6, [En ligne]. https://www.cdpdj.qc.ca/storage/app/media/publications/verification_police_clientele_vulnerable.pdf
COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Commentaires relatifs au projet de règlement modifiant le Règlement sur les centres de la petite enfance*, Me Claire BERNARD, (Cat. 2.412.98), 2003, p. 7 [En ligne]. https://www.cdpdj.qc.ca/storage/app/media/publications/commentaires_reglement_CPE.pdf

contenir des informations sensibles, par exemple l'état de santé mentale d'une personne lors d'une intervention[389]. Dans ses *Commentaires sur le 6e rapport quinquennal de la Commission d'accès à l'information*, elle soulignait de surcroît que :

> [L] e stigmate associé à la présence d'un antécédent judiciaire touche encore plus particulièrement certains groupes de la population, notamment en fonction des motifs de discrimination condition sociale, « race », couleur, origine ethnique ou nationale établis à l'article 10 de la Charte ou de l'intersectionnalité de ces motifs. Retenons à cet égard que les profilages racial et social visent certains groupes de personnes, notamment les personnes racisées, les Autochtones, les personnes en situation de pauvreté ou itinérantes de même que les personnes qui cumulent plusieurs de ces caractéristiques personnelles. La surveillance ciblée dont elles font l'objet de la part des services de police entraîne notamment les interpellations et arrestations disproportionnées ou abusives de même que la surjudiciarisation[390] et, éventuellement, un ou des antécédents judiciaires. Il faut d'ailleurs référer à ce sujet aux travaux de la Commission de vérité et de réconciliation du Canada dont l'un des appels à l'action vise l'élimination de la surreprésentation des Autochtones en détention au cours de la prochaine décennie.[391]

Ce stigmate peut avoir l'effet de limiter l'accès à l'emploi ou à d'autres services[392]. La Commission appuie donc à nouveau la recommandation de la CAI à l'effet de prévoir un encadrement législatif précis pour la vérification des antécédents judiciaires[393].

Rappelons que l'article 18.2 de la Charte encadre la vérification des antécédents judiciaires dans le cadre de l'emploi. De plus, la collecte et l'utilisation des antécédents judiciaires sont susceptibles de porter atteinte au droit au respect de sa vie privée et au droit à la sauvegarde de sa réputation de la personne concernée dans différents contextes.

---

389 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *La divulgation d'informations relatives à la santé mentale contenues dans les dossiers de police dans les cadre d'enquêtes d'antécédents judiciaires*, 2018. Voir COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Rapport d'activités et de gestion 2018-2019*, p. 54.

390 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Profilage racial et discrimination systémique des jeunes racisés*, préc., note 136; COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *La judiciarisation des personnes itinérantes à Montréal : un profilage social*, préc., note 137.

391 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc.,21, p. 18, COMMISSION DE VÉRITÉ ET DE RÉCONCILIATION DU CANADA, *Commission de vérité et de réconciliation du Canada : Appels à l'action*, Winnipeg, 2012, p. 4, [En ligne]. http://www.trc.ca/websites/trcinstitution/File/2015/Findings/Calls_to_Action_French.pdf

392 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 21, p. 18.

393 *Id.*, p. 17.

De l'avis de la Commission, le projet de loi nº 64 devrait proposer une définition plus précise de ce que constitue un renseignement sensible en tenant compte de ces exemples. Cette définition devrait en outre tenir compte des 14 motifs de discrimination prohibés par l'article 10 de la Charte[394]. À titre comparatif, le RGPD propose une définition plus précise de ce que constitue un renseignement sensible à son article 9 :

> Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

RECOMMANDATION 9

> **La Commission recommande que le projet de loi prévoie une définition plus précise de ce que constitue un renseignement sensible en tenant compte, entre autres, des motifs de discrimination prohibés par la Charte.**

3.3 Le consentement des personnes mineures

Le projet de loi introduirait dans la Loi sur le public et la Loi sur le privé des dispositions spécifiques sur le consentement des mineurs. Désormais, il serait prévu que :

> Un consentement prévu à la présente loi doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Il est demandé à chacune de ces fins, en termes simples et clairs, distinctement de toute autre information communiquée à la personne concernée. Lorsque celle-ci le requiert, il lui est prêté assistance afin de l'aider à comprendre la portée du consentement demandé.
>
> Le consentement du mineur de moins de 14 ans est donné par le titulaire de l'autorité parentale. Le consentement du mineur de 14 ans et plus est donné par le mineur ou par le titulaire de l'autorité parentale.
>
> […].[395]

Cependant, une exception à ce principe est prévue pour la collecte des renseignements personnels :

---

394 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 13, p. 14.

395 Projet de loi nº 64, art. 9, 102

> Les renseignements personnels concernant un mineur de moins de 14 ans ne peuvent être recueillis auprès de celui-ci sans le consentement du titulaire de l'autorité parentale, sauf lorsque cette collecte est manifestement au bénéfice de ce mineur.[396]

Comme mentionné plus haut, l'utilisation de services en ligne peut participer au développement et à l'autonomie des personnes mineures ainsi qu'à leur droit à la liberté d'expression et à l'information[397]. Parallèlement, les droits des personnes mineures sont susceptibles d'être affectés par la collecte et le traitement de leurs renseignements personnels. Leur vulnérabilité peut augmenter ce risque en plus de créer des risques d'atteinte qui leur sont propres. Des atteintes peuvent notamment résulter du fait d'un parent qui partage des renseignements personnels au sujet de son enfant. L'impossibilité de consentir des personnes mineures pourra aussi avoir des impacts sur leur liberté d'expression et leur droit au respect de la vie privée, dans les cas où le consentement du titulaire de l'autorité sera recherché. De plus, dans certaines situations, la nécessité d'obtenir le consentement d'un titulaire de l'autorité parentale pourrait mettre en péril le droit du mineur à la sûreté et à l'intégrité de sa personne ainsi que le droit à la sauvegarde de sa dignité. On pense particulièrement aux mineurs LGBTQIA2[398] et à ceux vivant une situation de violence familiale[399]. Pour pallier ce risque, le RGPD prévoit une exception « dans le cadre de services de prévention ou de conseil proposés directement à un enfant. »[400] L'exception proposée dans le projet de loi pourrait aussi pallier ce risque.

La complexité de la conciliation entre le droit à la protection des personnes mineures et le respect de leur autonomie et leurs droits révèle l'importance d'incorporer dans la protection de leurs renseignements personnels deux principes fondamentaux : la considération primordiale que constitue l'intérêt de l'enfant dans toute décision le concernant[401] et le droit de l'enfant d'exprimer son opinion sur toute question l'intéressant et d'être entendu dans toute procédure

---

396 *Id*., art. 16, 96.

397 Voir *supra*, section 2.1.3.

398 D. KEATS CITRON, préc., note 83.

399 M. MACENAITE et E. KOSTA, préc., note 78, p. 163.

400 RGPD, 38^e^ considérant du Préambule.

401 *Convention relative aux droits de l'enfant*, 20 novembre 1989, R.T. Can. 1992, art. 3 al. 1 (ci-après « Convention relative aux droits de l'enfant ». Voir à ce sujet : COMITÉ DES DROITS DE L'ENFANT, *Observation générale n^o^ 14 (2013) sur le droit de l'enfant à ce que son intérêt supérieur soit une considération primordiale (art. 3, par. 1)*, Doc. N.U. CRC/C/GC/14.

judiciaire ou administrative l'intéressant[402]. Or, ni la Loi sur le public ni la Loi sur le privé n'incorporent ces principes. Le *Code civil du Québec*[403] et la *Loi sur la protection de la jeunesse*[404] reconnaissent déjà ces deux grands principes directeurs en matière de droits de l'enfant[405] et la Commission recommande depuis plusieurs années leur reconnaissance en matière de protection des renseignements personnels[406]. Ces principes devraient notamment toujours participer à la décision d'un titulaire de l'autorité parentale de donner le consentement pour un enfant dont il est responsable. Nous soulignons aussi l'importance de ces principes dans les cas où il y aurait un conflit entre le désir de consentir d'un enfant de 14 ans et plus et celui du titulaire de l'autorité parentale. La Commission recommande donc que ces principes soient reconnus dans les deux lois.

RECOMMANDATION 10

> **La Commission recommande que le projet de loi nº 64 soit modifié afin que l'intérêt de l'enfant dans toute décision le concernant ainsi que le droit de l'enfant d'exprimer son opinion sur toute question l'intéressant et d'être entendu dans toute procédure judiciaire ou administrative l'intéressant soient reconnus dans la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels dans le secteur privé*.**

Rappelons que le droit québécois accorde aux personnes mineures un « accès graduel à l'autonomie[407]. » On reconnaît par ailleurs que leur capacité de discernement, « qui dépend notamment [du] niveau de développement intellectuel, moral et émotif »[408], évolue avec l'âge.

---

402 *Convention relative aux droits de l'enfant*, art. 12. Voir à ce sujet : COMITÉ DES DROITS DE L'ENFANT, *Observation générale nº 12 (2009) sur le droit de l'enfant d'être entendu*, Doc. N.U. CRC/C/GC/12.

403 Notamment à ses articles 33 et 34.

404 *Loi sur la protection de la jeunesse*, préc., note 3, art. 2.4, par. 4º, 6, 7, 74.2 et 80.

405 Voir à ce sujet : C. BERNARD, préc., note 228, p. 25.

406 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 94, p. 31; COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 345; COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Mémoire à la Commission de la culture de l'Assemblée nationale Examen du Rapport quinquennal de la Commission d'accès à l'information, Une réforme de l'accès à l'information : le choix de la transparence*, (Cat. 2.412.42.2), 2003, p. 6-7, [En ligne]. https://www.cdpdj.qc.ca/storage/app/media/publications/memoire_rapport_CAI.pdf et COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Les droits de l'enfant et des parents sur les dossiers qui concernent l'enfant : exposé descriptif*, Me Claire BERNARD, (Cat. 2.176.5), 2003, p.8.

407 C. BERNARD, préc., note 228, p.26.

408 *Id.*, p. 30-31.

Cette capacité a une influence les termes qu'une personne mineure est en mesure de comprendre, notamment en ce qui concerne l'utilisation de ses renseignements. Or, le principe du consentement éclairé exige que la capacité de discernement des personnes mineures soit prise en compte lors de l'obtention de leur consentement[409]. Par exemple, la *Loi sur la protection de la jeunesse* prévoit que :

> 2.4. Les personnes à qui la présente loi confie des responsabilités envers l'enfant ainsi que celles appelées à prendre des décisions à son sujet en vertu de cette loi tiennent compte, lors de leurs interventions, de la nécessité:
> […]
>
> 2° de s'assurer que les informations et les explications qui doivent être données à l'enfant dans le cadre de la présente loi doivent l'être en des termes adaptés à son âge et à sa compréhension; […].

RECOMMANDATION 11

> **La Commission recommande que le projet de loi nº 64 prévoie que les informations données à la personne mineure lors de l'obtention de son consentement soient adaptées à son âge et sa compréhension.**

Le projet de loi ne précise pas comment doit être effectuée la vérification de l'âge et du consentement des titulaires de l'autorité parentale. Il s'agit d'une question qui ne fait pas l'unanimité. Certaines méthodes s'avèrent trop faciles à contourner ou autrement inefficaces[410]. Conséquemment, la protection des renseignements personnels des personnes mineures ainsi que des droits sous-jacents devient plutôt théorique. Il serait donc pertinent que les mécanismes de vérification d'âge et du consentement des titulaires de l'autorité parentale soient encadrés de manière plus précise[411].

Finalement, force est de constater qu'il est important de sensibiliser les personnes mineures aux enjeux relatifs à la collecte et à l'utilisation de leurs renseignements personnels. Comme l'a

---

409 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA , « Projet de position du Commissariat sur la réputation en ligne » (26 janvier 2018), [En ligne]. https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-sur-la-reputation-en-ligne/pos_or_201801/ (consulté le 1er septembre 2020). Voir aussi : COMITÉ DES DROITS DE L'ENFANT, préc., note 402, par. 25 et 48.

410 M. MACENAITE et E. KOSTA préc., note 77, p. 181.

411 *Id*.

déjà affirmé la Commission dans les contextes d'éducation et de sensibilisation, « un arrimage plus explicite avec le cadre des droits et libertés pourrait apporter un éclairage pertinent »[412].

3.4 L'évaluation des facteurs relatifs à la vie privée

Le projet de loi introduirait la notion « d'évaluation des facteurs relatifs à la vie privée » à plusieurs endroits dans la Loi sur le public et dans la Loi sur le privé.

Par exemple, le projet de loi nº 64 introduirait des articles dans la Loi sur le public qui se liraient comme suit :

> 63.5. Un organisme public doit procéder à une évaluation des facteurs relatifs à la vie privée de tout projet de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.
>
> Aux fins de cette évaluation, l'organisme public doit consulter, dès le début du projet, son comité sur l'accès à l'information et la protection des renseignements personnels.
>
> Cet organisme public doit également s'assurer que ce projet permet qu'un renseignement personnel informatisé recueilli auprès de la personne concernée soit communiqué à cette dernière dans un format technologique structuré et couramment utilisé.[413]
>
> 67.2.1. Un organisme public peut communiquer des renseignements personnels sans le consentement des personnes concernées à une personne ou à un organisme qui souhaite utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques.
>
> La communication peut s'effectuer si une évaluation des facteurs relatifs à la vie privée conclut que :
>
> 1° l'objectif de l'étude, de la recherche ou de la production de statistiques ne peut être atteint que si les renseignements sont communiqués sous une forme permettant d'identifier les personnes concernées;
>
> 2° il est déraisonnable d'exiger que la personne ou l'organisme obtienne le consentement des personnes concernées;
>
> 3° l'objectif de l'étude, de la recherche ou de la production de statistiques l'emporte sur l'impact de la communication et de l'utilisation des renseignements sur la vie privée des personnes concernées;
>
> 4° les renseignements personnels sont utilisés de manière à en assurer la confidentialité;

---

412 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Mémoire : consultations sur le programme d'études Éthique et culture religieuse*, (Cat. 2.120-4.22.1), 2020, p. 47 [En ligne]. https://cdpdj.qc.ca/storage/app/media/publications/memoire_ECR.pdf

413 Projet de loi nº 64, art 14.

5° seuls les renseignements nécessaires sont communiqués.[414]

70.1. Avant de communiquer à l'extérieur du Québec un renseignement personnel, un organisme public doit procéder à une évaluation des facteurs relatifs à la vie privée. Il doit notamment tenir compte des éléments suivants :

1° la sensibilité du renseignement;

2° la finalité de son utilisation;

3° les mesures de protection dont le renseignement bénéficierait;

4° le régime juridique applicable dans l'État où ce renseignement serait communiqué, notamment son degré d'équivalence par rapport aux principes de protection des renseignements personnels applicables au Québec.

La communication peut s'effectuer si l'évaluation démontre que le renseignement bénéficierait d'une protection équivalant à celle prévue à la présente loi. Elle doit faire l'objet d'une entente écrite qui tient compte notamment des résultats de l'évaluation et, le cas échéant, des modalités convenues dans le but d'atténuer les risques identifiés dans le cadre de cette évaluation.

Il en est de même lorsque l'organisme public confie à une personne ou à un organisme à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour son compte un tel renseignement.

Le présent article ne s'applique pas à une communication prévue au paragraphe 4° du deuxième alinéa de l'article 59 ou au paragraphe 1.1° du premier alinéa de l'article 68. Il ne s'applique pas non plus à une communication faite dans le cadre d'un engagement international visé au chapitre III de la Loi sur le ministère des Relations internationales (chapitre M-25.1.1), à une communication faite dans le cadre d'une entente visée au chapitre III.1 ou III.2 de cette loi ou à une communication prévue à l'article 133 de la Loi sur la santé publique (chapitre S-2.2).

70.4. Un gestionnaire de renseignements personnels doit, avant de recueillir, utiliser ou communiquer des renseignements personnels dans l'exercice de sa fonction, procéder à une évaluation des facteurs relatifs à la vie privée et la transmettre à la Commission.

Ce gestionnaire doit également établir des règles encadrant sa gouvernance à l'égard des renseignements personnels et les faire approuver par la Commission. Ces règles doivent notamment prévoir l'encadrement applicable à la conservation et à la destruction de ces renseignements, prévoir les rôles et les responsabilités des membres de son personnel tout au long du cycle de vie de ces renseignements et un processus de traitement des plaintes relatives à la protection de ceux-ci. Ces règles doivent être à nouveau soumises pour approbation à la Commission tous les deux ans.

Ces règles sont publiées sur le site Internet du gestionnaire, dans une section dédiée à sa fonction.[415]

414 *Id.*, art. 23.

415 *Id.*, art. 27.

D'autres articles de la loi actuelle seraient modifiés pour introduire la notion d'« évaluation des facteurs relatifs à la vie privée »[416].

Cette notion serait également introduite à la Loi sur le privé[417].

La Commission note que cette évaluation est faite par le détenteur des informations. Il n'est pas prévu qu'elle fasse l'objet d'une révision par un organisme indépendant. Or, d'après deux membres du Sénat du Canada, l'autorégulation en matière de protection des renseignements personnels a montré ses limites[418]. Dans d'autres domaines, une analyse a démontré que l'autorégulation n'était pas adéquate ni effective comme moyen de garantir que les entreprises transnationales respectent les droits de la personne[419]. La professeure Erika George estime pour sa part qu'il est nécessaire d'encadrer les activités de reddition de compte des entreprises dans le domaine des technologies de l'information pour renforcer la protection des droits de la personne[420].

De l'avis de la Commission, le fait que l'évaluation soit faite par l'entité qui détient les informations et qui a intérêt à les exploiter sans supervision externe la rend insuffisante pour garantir que les droits des personnes concernées par ces renseignements sont garantis. À titre d'exemple, le RGPD prévoit que le responsable du traitement au sein d'une organisation consulte l'autorité de contrôle publique indépendante de son État lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé[421].

---

416 *Id.*, art. 15 qui modifierait l'article 64 de la Loi sur le public et art. 25 qui modifierait l'article 68 de la Loi sur le public.

417 Loi sur le privé, art. 95, 103, 110 et 117.

418 Art EGGLETON et Raymonde SAINT-GERMAIN, « Il est temps de resserrer les lois canadiennes sur la protection de la vie privée afin qu'elles tienne compte de l'évolution des technologies », *Options politiques*, 2 juillet 2018, [En ligne]. https://policyoptions.irpp.org/magazines/july-2018/ameliorer-la-protection-des-donnees-personnelles-au-canada/

419 Penelope SIMONS, « Corporate Voluntarism and Human Rights: The Adequacy of Voluntary Self-Regulation Regimes », (2004) 59:1 *Relations industrielles* 101, 129.

420 Erika GEORGE, « Corporate Social Responsibility and Social Media Corporations: Incorporating Human Rights through Rankings, Self-Regulation and Shareholder Resolutions » (2018) 28:3 *Duke Journal of Comparative & International Law* 521, p. 538.

421 RGPD, art. 35.

RECOMMANDATION 12

> **La Commission recommande que le projet de loi nº 64 prévoie que l'évaluation des impacts relatifs à la vie privée fasse l'objet d'une supervision externe par un tiers indépendant.**

Si cette supervision externe par un tiers indépendant permettrait d'espérer une amélioration de la protection du droit au respect de sa vie privée dans tous ses aspects, elle ignorerait cependant les autres droits garantis par le Charte qui sont susceptibles d'être compromis par le fait de recueillir, de traiter, de partager et de conserver des renseignements personnels.

De fait, la Commission a indiqué à plusieurs reprises que « l'utilisation d'une innovation technologique constituera un progrès seulement si les impacts de cette technologie sur les droits de la personne ont été évalués. Les développements technologiques ne devraient pas entraîner un renoncement à la protection des droits fondamentaux.»[422]

RECOMMANDATION 13

> **La Commission recommande que soit remplacée l'expression « facteurs relatifs à la vie privée » par celle de « facteurs relatifs aux droits et libertés de la personne garantis par la Charte », et ce, dans l'ensemble du projet de loi.**

En outre, il pourrait être utile de spécifier que la Loi sur le public et la Loi sur le privé tirent leur caractère législatif fondamental de leur lien avec les dispositions de la Charte.

RECOMMANDATION 14

> **La Commission recommande que le projet de loi nº 64 réfère aux droits et libertés de la personne garantis par la Charte.**

3.5 La notion d'anonymisation

Le projet de loi nº 64 introduirait la notion d'« anonymisation » à la Loi sur le public et à la Loi sur le privé.

---

422 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 14; COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 13; COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 10. [Renvoi omis].

Par exemple, l'article 28 du projet de loi nº 64 modifierait l'article 73 de la Loi sur le public de la façon suivante :

> 73. Lorsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, l'organisme public doit le détruire ou l'anonymiser, sous réserve de la Loi sur les archives (chapitre A-21.1) ou du Code des professions (chapitre C-26).
>
> Pour l'application de la présente loi, un renseignement concernant une personne physique est anonymisé lorsqu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne.
>
> Les renseignements anonymisés en vertu de la présente loi doivent l'être selon les meilleures pratiques généralement reconnues.[423]

Le projet créerait également une infraction à la Loi sur le public contre les tentatives d'identifier à nouveau les personnes :

> 159. Commet une infraction et est passible d'une amende de 5 000 $ à 50 000 $ dans le cas d'une personne physique et de 15 000 $ à 150 000 $ dans les autres cas quiconque :
>
> […]
>
> 2° procède ou tente de procéder à l'identification d'une personne physique à partir de renseignements dépersonnalisés sans l'autorisation de l'organisme public qui les détient ou à partir de renseignements anonymisés;
>
> […].[424]

De même, la Loi sur le privé serait modifiée afin de permettre l'anonymisation plutôt que la destruction à l'expiration du délai de conservation. L'article 23 de la loi actuelle serait remplacé par le suivant :

> 23. Lorsque les fins auxquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, la personne qui exploite une entreprise doit le détruire ou l'anonymiser, sous réserve d'un délai de conservation prévu par une loi.
>
> Pour l'application de la présente loi, un renseignement concernant une personne physique est anonymisé lorsqu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne.
>
> Les renseignements anonymisés en vertu de la présente loi doivent l'être selon les meilleures pratiques généralement reconnues.[425]

---

423 Loi sur le public, art. 73 tel qu'il serait modifié par l'art. 28 du projet de loi nº 64 (les ajouts sont soulignés).

424 Projet de loi nº 64, art. 64.

425 *Id.*, art. 111.

L'anonymisation différerait de la dépersonnalisation qui se définirait comme suit :

> […] Pour l'application de la présente loi, un renseignement personnel est :
>
> 1° dépersonnalisé lorsque ce renseignement ne permet plus d'identifier directement la personne concernée; […].[426]

Or comme la Commission l'a déjà indiqué :

> Au regard des travaux sur la question, la Commission est d'avis qu'une anonymisation ou qu'une dé-identification parfaite sont difficiles à concevoir. Étant donné les risques de réidentification, les données devraient continuer à être considérées comme des renseignements personnels.[427]

RECOMMANDATION 15

> **La Commission recommande que la notion d'anonymisation ne soit pas introduite au projet de loi nº 64.**

3.6 Le droit à la rectification

En remplaçant l'article 28 de la Loi sur le privé, le projet de loi créerait la possibilité de faire rectifier un renseignement s'il est « inexact, incomplet ou équivoque » ou si « la collecte, la communication ou la conservation ne sont pas autorisées par loi ».

La possibilité de faire rectifier un renseignement dont la collecte, la communication ou la conservation ne sont pas autorisées par la loi s'ajouterait aux droits déjà prévus au Code civil[428] de faire corriger des renseignements inexacts, incomplets ou équivoques dans un dossier.

La Commission a, à plusieurs reprises, souligné l'importance du droit à la rectification des renseignements personnels, notamment lorsque des décisions sont prises sur la base de ceux-

---

426 Loi sur le privé, art. 12 qui serait introduit par l'art. 102 du projet de loi nº 64; Voir également l'art. 65.1 de la Loi sur le public tel qu'il serait modifié par l'art. 19 du projet de loi nº 64.

427 COMMISSION DES DROITS DE LA LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 13, p. 24.

428 L'article 40 du *Code civil* prévoit :

> 40. Toute personne peut faire corriger, dans un dossier qui la concerne, des renseignements inexacts, incomplets ou équivoques; elle peut aussi faire supprimer un renseignement périmé ou non justifié par l'objet du dossier, ou formuler par écrit des commentaires et les verser au dossier.

ci[429]. Le droit à la rectification participe notamment du droit à l'information et au droit à la sauvegarde de sa dignité de son honneur et de sa réputation[430]. La Commission salue donc cette modification.

La Commission rappelle aussi que puisqu'un renseignement personnel inféré devrait être considéré comme un renseignement personnel, le droit à la rectification devrait aussi s'appliquer à tout renseignement inféré[431].

3.7 Le « droit à l'oubli »

Le projet de loi prévoit un nouvel article 28.1 dans la Loi sur le privé qui cristalliserait notamment un « droit à l'oubli » :

> 28.1. La personne concernée par un renseignement personnel peut exiger d'une personne qui exploite une entreprise qu'elle cesse la diffusion de ce renseignement ou que soit désindexé tout hyperlien rattaché à son nom permettant d'accéder à ce renseignement par un moyen technologique, lorsque la diffusion de ce renseignement contrevient à la loi ou à une ordonnance judiciaire.
>
> Elle peut faire de même, ou encore exiger que l'hyperlien permettant d'accéder à ce renseignement soit réindexé, lorsque les conditions suivantes sont réunies :
>
> 1° la diffusion de ce renseignement lui cause un préjudice grave relatif au droit au respect de sa réputation ou de sa vie privée;
>
> 2° ce préjudice est manifestement supérieur à l'intérêt du public de connaître ce renseignement ou à l'intérêt de toute personne de s'exprimer librement;
>
> 3° la cessation de la diffusion, la réindexation ou la désindexation demandée n'excède pas ce qui est nécessaire pour éviter la perpétuation du préjudice.
>
> Dans l'évaluation des critères du deuxième alinéa, il est tenu compte, notamment :
>
> 1° du fait que la personne concernée est une personnalité publique;
>
> 2° du fait que la personne concernée est mineure;
>
> 3° du fait que le renseignement est à jour et exact;
>
> 4° de la sensibilité du renseignement;
>
> 5° du contexte dans lequel s'effectue la diffusion du renseignement;

---

429 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 11; COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 10, p. 18.

430 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 13, p. 18-19.

431 *Id.*, p. 13.

> 6° du délai écoulé entre la diffusion du renseignement et la demande faite en vertu du présent article;
>
> 7° si le renseignement concerne une procédure criminelle ou pénale, de l'obtention d'un pardon ou de l'application d'une restriction à l'accessibilité des registres des tribunaux judiciaires.
>
> Les articles 30, 32 et 34 s'appliquent à une demande faite en vertu du présent article, avec les adaptations nécessaires.

La possibilité de contacter l'exploitant d'une entreprise pour faire cesser la diffusion d'un renseignement qui contrevient à la loi ou à une ordonnance judiciaire est susceptible d'améliorer l'accès à la justice et la protection des droits à la sauvegarde à la réputation et de sa dignité et au respect de sa vie privée en créant un recours supplémentaire visant directement l'entreprise.

Le droit à l'oubli, plus exactement appelé « droit au déréférencement » ou « droit à la désindexation » dans le cas présent, s'est d'abord développé en Europe[432] et fait l'objet de discussions au Canada et au Québec depuis quelques années[433]. Selon le Commissariat à la protection de la vie privée du Canada, « [l] e déréférencement est le processus par lequel une page Web, une image ou une autre ressource en ligne est supprimée des résultats présentés par un moteur de recherche lorsque l'utilisateur a entré le nom d'une personne comme terme de recherche[434]. »

On peut voir des liens entre ce nouveau « droit » et les principes établis en matière de droit d'accès[435] et de rectification[436] qui participent du droit au respect de sa vie privée[437].

---

432 *Google Spain SL, Google Inc c Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez,* Cour de Justice de l'Union européenne (Grande Chambre), affaire C-131/12. 13 mai 2014, RGPD*,* art. 17.

433 Geneviève SAINT-LAURENT, « Vie Privée et Droit à l'Oubli: Que Fait le Canada », (2015) 66 *U.N.B.L.J.* 185.

434 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Projet de position du Commissariat sur la réputation en ligne » (26 janvier 2018), [En ligne]. https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-sur-la-reputation-en-ligne/pos_or_201801/ (consulté le 1er septembre 2020).

435 Loi sur le public, art. 83; Loi sur le privé, art. 27.

436 Voir supra section 3.6

437 *Alberta (Information and Privacy Commissioner)* c. *Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401*, préc., note 167 , par. 24.

Le droit à la désindexation est susceptible d'affecter plusieurs droits et libertés garantis à la Charte, notamment le droit au respect de sa vie privée, le droit à la sauvegarde de son honneur, sa réputation et sa dignité, le droit à la liberté d'expression et le droit à l'information. Par ailleurs, certains aspects de l'article proposé méritent d'être commentés plus précisément.

3.7.1 Les conflits de droits

Dans bien des cas, une demande de désindexation créera un conflit de droits[438], par exemple le droit à la sauvegarde de la dignité d'un individu et le droit à la liberté d'expression de celui qui partage le renseignement personnel. Cela pourrait aussi opposer le droit au respect de sa vie privée d'un individu et le droit à l'information du public. Il y a lieu de saluer l'approche au cas par cas qui serait adoptée en vertu du projet de loi, qui est susceptible de permettre l'atteinte d'un équilibre entre les divers droits qui entreront en conflit.

La Commission a déjà rappelé que ce genre d'« exercice de conciliation devrait tenir compte des principes de résolution des conflits de droits et des règles régissant l'interprétation des droits de la personne »[439].

En vertu du projet de loi, la CAI sera l'organisme chargé de réviser les décisions des entreprises en cas de désaccord sur une demande de désindexation[440]. Or, comme mentionné, ces décisions mettent en jeu des droits protégés par la Charte, dont plusieurs peuvent entrer en conflit. Dans son *Mémoire à la Commission de la culture sur le projet de loi nº 451*, la Commission s'est dite préoccupée que le mandat de la CAI en demeure un de surveillance et contrôle des renseignements personnels et ne visant pas explicitement la promotion et la protection des droits sous-jacents aux lois qu'elle applique, malgré la prépondérance des droits de la Charte et l'importance d'assurer la promotion de ses principes[441]. La Commission souligne

---

438 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 434, COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 21, p. 21-22

439 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *id.*, p. 11.

440 Projet de loi nº 64, art. 123.

441 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Mémoire à la Commission de la culture sur le projet de loi 451, Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels dans le secteur privé et d'autres dispositions législatives*, (Cat. 2.412-42.2), 1998, p. 7-8 [En ligne]. https://cdpdj.qc.ca/storage/app/media/publications/pl451_acces.pdf

donc à nouveau que toute instance, incluant la CAI, est tenue de prendre en compte les droits prévus par la Charte[442].

3.7.2 Commentaires sur des critères particuliers

Il y a lieu de se pencher sur certains éléments d'évaluation prévus par le projet de loi pour aider le décideur à déterminer si le « préjudice est manifestement supérieur à l'intérêt du public de connaître ce renseignement ou à l'intérêt de toute personne de s'exprimer librement »[443].

La Commission salue par ailleurs les éléments suivants, dont certains sont conformes aux recommandations du Commissariat à la protection de la vie privée du Canada[444], soit :

- le fait que la personne concernée est une personnalité publique;
- le fait que la personne concernée est mineure;
- la sensibilité du renseignement;
- le fait que le renseignement concerne une procédure criminelle ou pénale, de l'obtention d'un pardon ou de l'application d'une restriction à l'accessibilité des registres des tribunaux judiciaires.

Au sujet de ce dernier critère, la Commission rappelle à nouveau la discrimination, particulièrement dans l'embauche, dont font l'objet les personnes ayant des antécédents judiciaires, discrimination qui est souvent croisée avec d'autres motifs tels la « race », l'origine ethnique, la condition sociale ou le handicap, un motif qui peut inclure les problèmes de santé mentale[445].

La Commission formule de plus les commentaires suivants.

---

442 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 145 citant COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE (2015), préc., note 166, p. 30

443 Loi sur le privé, art. 28.1, al. 2, par. 2, qui serait introduit par projet de loi nº 64, art. 113.

444 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 434.

445 Voir *supra*, section 3.2.4.

Les renseignements concernant les personnes mineures

La décision de cesser de diffuser, de désindexer ou de réindexer un renseignement doit tenir compte « du fait que la personne concernée est mineure ».

À l'instar du Commissariat à la protection de la vie privée du Canada, nous sommes d'avis que « [les enfants et les adolescents] sont aussi dans une période d'expérimentation au cours de laquelle ils testent les limites. Il est donc essentiel de donner aux jeunes un moyen de se réinventer à mesure qu'ils évoluent et entrent dans l'âge adulte »[446].

La Commission salue d'abord ce critère, qui devrait peser en faveur d'une désindexation.

Cette possibilité de se réinventer, qui participe notamment des droits au respect de la vie privée et à la sauvegarde de la dignité des personnes mineures, pourrait être limitée par les renseignements personnels partagés notamment par les titulaires de l'autorité parentale[447]. Cette atteinte pourrait d'ailleurs se perpétuer au-delà de l'âge de la majorité[448]. Il en va aussi du droit à la liberté de sa personne, puisqu'une personne devrait être libre de choisir l'ampleur de sa présence en ligne. Or, telle qu'elle est rédigée, la disposition proposée semble favoriser la désindexation seulement lorsqu'une personne mineure ou son représentant en fait la demande. La Commission est d'avis que, même une fois l'âge de la majorité atteint, une personne devrait pouvoir faire désindexer les renseignements personnels partagés alors qu'elle était mineure.

RECOMMANDATION 16

> **La Commission recommande que l'alinéa 3 (2°) de l'article 28.1 de la *Loi sur la protection des renseignements personnels dans le secteur privé*, qui serait introduit par l'article 113 du projet de loi nº 64, soit remplacé par « du fait que la personne concernée était mineure au moment de la diffusion ».**

---

446 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 434.

447 Voir *supra* section 2.1.3.

448 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 434.

Les renseignements inexacts

Le projet de loi prévoit qu'il doit être tenu compte « du fait que le renseignement est à jour et exact ».

La Commission déduit que l'exactitude d'un renseignement milite, notamment du point de vue du droit à l'information, en faveur de l'intérêt du public à le connaître. Il y a cependant lieu de se questionner sur une interprétation *a contrario* de cet article. En effet, l'exactitude n'est qu'un élément à considérer dans une demande en vertu du nouvel article 28.1 de la Loi sur le privé. On pourrait donc interpréter qu'il serait possible de refuser une demande même si les renseignements personnels visés sont inexacts. Cela pourrait engendrer des atteintes au droit au respect de sa vie privée et au droit à la sauvegarde de sa réputation et de sa dignité, en plus de contrevenir au droit à la rectification proposé à l'article précédent. La Commission recommande donc une clarification de cet élément.

RECOMMANDATION 17

> **La Commission recommande de modifier l'article 113 du projet de loi nº 64 qui introduirait l'article 28.1 al. 3.3 dans la *Loi sur la protection des renseignements personnels dans le secteur privé* pour clarifier qu'il vise à protéger les renseignements exacts, sans porter atteinte au droit de faire rectifier les renseignements inexacts.**

3.8 Les sanctions administratives pécuniaires

Le projet de loi nº 64 prévoit l'introduction d'une section à la Loi sur le privé qui s'intitulerait « Sanctions administratives pécuniaires »[449]. Elle prévoit, comme son nom l'indique, l'imposition de sanctions administratives pécuniaires en cas de contravention à certaines dispositions de loi. Le montant maximal de ces sanctions administratives serait « de 50 000 $ dans le cas d'une personne physique et, dans les autres cas, de 10 000 000 $ ou du montant correspondant à 2 % du chiffre d'affaires mondial de l'exercice financier précédent si ce dernier montant est plus élevé »[450]. Il s'agit de montants substantiels en comparaison des montants actuels des

449 Projet de loi nº 64, art. 150.

450 Loi sur le privé, art. 90.12 qui serait introduit par projet de loi nº 64, art. 150.

amendes pour les infractions réglementaires qui atteignent actuellement un maximum de 100 000 $ en cas de récidive[451].

Nous sommes d'avis qu'il est nécessaire de renforcer les sanctions en ce qui concerne les violations de la Loi sur le privé en vue d'affermir la mise en œuvre des droits garantis par la Charte. Par exemple, dans son mémoire sur les applications de notification de contacts, la Commission a recommandé que le gouvernement adopte des mesures « effectives »[452].

Cependant, le recours à des sanctions administratives pécuniaires plutôt qu'à des infractions réglementaires ou des infractions pénales soulève des risques de violations des droits judiciaires garantis par la Charte.

La jurisprudence de la Cour suprême reconnaît la validité de ce type de sanctions qui ne donnent pas accès au bénéfice de la procédure pénale, entre autres, spécifiquement dans le domaine disciplinaire[453]. Cette cour a réitéré les critères alternatifs qu'elle avait élaborés à l'occasion de décisions précédentes en vue de décider si une infraction devrait être soumise à des garanties procédurales constitutionnelles :

> Le critère de la nature criminelle permet de circonscrire les dispositions qui sont de nature criminelle du fait que le Parlement ou la législature a établi une procédure dont les attributs et l'objet montrent que la sanction est infligée à l'issue d'une procédure de nature criminelle. Par contre, le critère de la véritable conséquence pénale consiste à se demander si une disposition d'apparence administrative ou réglementaire donne néanmoins droit aux protections de l'art. 11 de la *Charte* [canadienne] parce que son application peut entraîner une conséquence pénale. Un certain chevauchement est inévitable, mais il importe de prendre en compte toutes les considérations pertinentes et de se rappeler que les deux volets du critère ne conduisent que rarement à des conclusions différentes (comme dans *Wigglesworth*).[454]

451 Loi sur le privé, art. 91.

452 COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, préc., note 14, recommandation 7.

453 *R.* c. *Wigglesworth*, [1987] 2 RCS 541, 1987 CanLII 41 (CSC)

454 *Guindon* c. *Canada*, 2015 CSC 41, par. 49.

Or ces critères ont soulevé la critique en raison, entre autres, de leur manque de clarté[455]. Comme l'indique la professeure Anne-Marie Boisvert :

> [I] l est impossible d'expliquer de manière rationnelle et cohérente la différence fondamentale que l'on voudrait établir entre les infractions pénales consécutives à la violation de la réglementation d'une activité légitime dans l'intérêt public, pour lesquelles certaines protections de nature constitutionnelle s'appliquent, et les manquements à la réglementation que l'on sanctionne dans le but de protéger l'intérêt public, et qui constituent des violations de type administratif auxquels la Charte ne s'applique pas.[456] [Renvois omis.]

On a également reproché aux sanctions administratives pécuniaires, à juste titre à notre avis, de permettre aux acteurs étatiques de se soustraire à l'obligation d'offrir les garanties judiciaires prévues à la Charte tout simplement en choisissant une procédure administrative[457]. La professeure Boivert indique :

> Il faut relever d'emblée la circularité évidente du raisonnement qui s'en remet au processus préconisé par le législateur comme élément permettant de déterminer le processus qui devrait être suivi. Autrement dit, on nous explique qu'en privilégiant l'efficacité administrative, le législateur peut par le fait même décider que la Charte, et les garanties procédurales qu'elle contient, ne lui impose aucune contrainte. Paradoxalement donc, moins un processus n'offre de garanties à la personne sanctionnée, moins il serait sujet à l'examen constitutionnel. La question devrait pourtant être de savoir si la Charte impose à l'État de respecter certaines garanties procédurales avant d'imposer la sanction, et non de savoir si le législateur entendait fournir ou non ces garanties.[458]

Puisque ce type de sanctions prive les mis en cause des garanties judiciaires normalement assorties à l'attribution d'une peine, en particulier la présomption d'innocence[459], le droit au

---

455 Doug MCLEOD, « Facing the Consequences : Should the Charter Apply to Administrative Proceedings Involving Monetary Penalties? », (2012) 30 *N.J.C.L.* 59p. 60 et Stephen AYLWARD et Luisa RITACCA, « In Defence of Administrative Law : Procedural Fairness for Administrative Monetary Penalties » (2015), 28 *C.J.A.L.P.* 35, 45.

456 Anne-Marie BOISVERT, « Les dérives du droit administratif : les régimes de sanctions administratives pécuniaires comme alternative au droit pénal », [2018] 23 *C.C.L.R.* 197, 200.

457 D. MCLEOD*,* préc., note 455, 84.

458 A.-M. BOISVERT, préc., note 456, 204-205.

459 Charte, art. 33.

silence[460] et le droit à une défense pleine et entière[461], le recours à des sanctions administratives pécuniaires ne devrait pas être permis. Comme l'indique la Professeure Boisvert :

> Il n'est pas question ici d'imposer sans nuances à l'État des obligations équivalentes à celles qui s'appliquent dans toute leur rigueur en matière criminelle chaque fois qu'on veut recourir à la sanction administrative pour faire respecter une loi donnée. Mais les critères constitutionnels devraient à tout le moins refléter le principe bien connu voulant que, plus les conséquences d'une décision ont des effets importants pour l'administré, plus les garanties qui lui sont consenties doivent être importantes.[462]

RECOMMANDATION 18

La Commission recommande que le projet de loi nº 64 recoure à des infractions administratives ou à des infractions pénales plutôt qu'à des sanctions administratives pécuniaires.

CONCLUSION

Dans le contexte social actuel où les comportements font office de données brutes gratuites que les entreprises privées exploitent par l'extraction, la vente et la prédiction. Ce faisant, elles influencent l'ensemble des facettes de la vie des personnes, notamment nos comportements de consommateurs et d'électeurs, mais plus largement de citoyens. En outre, employeurs et autorités publiques recourent aux technologies de l'information pour nous surveiller en contournant les balises posées par le droit.

Or, au Québec, le droit au respect de sa vie est un droit fondamental garanti par la Charte. À titre de droit de la personnalité, il ne devrait pas faire l'objet d'une exploitation commerciale.

460 *Id.*, art. 33.1.

461 *Id.*, art. 35.

462 A.-M. BOISVERT, préc., note 456, 232.

En outre, la collecte et l'utilisation des renseignements personnels sont susceptibles de compromettre plusieurs autres droits de la personne que nous avons énumérés dans ce mémoire.

La Commission est d'avis que le législateur devrait profiter de la refonte de la Loi sur le public et de la Loi sur le privé que constitue le projet de loi nº 64 pour s'assurer que l'ensemble des droits et libertés qui peuvent être affectés par la collecte et l'utilisation des renseignements personnels soient protégés. En effet, bien que le consentement soit la seule source légitime de renonciation aux droits et libertés garantis par la Charte, il apparaît aussi nécessaire que le cadre législatif garantisse que les usages qui sont faits des renseignements personnels recueillis soient conformes avec les dispositions de la Charte. De fait, les effets de l'exploitation commerciale des données sur les droits sont systémiques et le contrôle des données ne saurait reposer strictement sur la responsabilité individuelle. Ils commandent donc un encadrement législatif en phase avec l'évolution des nouvelles technologies.

Dans le peu de temps qu'il lui a été alloué pour faire l'analyse de ce projet de loi d'une importance capitale, la Commission formule les recommandations suivantes :

RECOMMANDATION 1

> **La Commission recommande de retirer le terme « exclusivement » de l'article 65.2 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* tel qu'il serait modifié par l'article 20 du projet de loi nº 64 et de l'article 12.1 de la *Loi sur la protection des renseignements personnels dans le secteur privé* tel qu'il serait introduit par l'article 102 du projet de loi nº 64.**

RECOMMANDATION 2

> **La Commission recommande que le projet de loi nº 64 prévoie que l'utilisation des renseignements personnels aux fins de prise de décision automatisée confère le droit à une intervention humaine ainsi que le droit de contester le résultat ainsi produit.**

RECOMMANDATION 3

> **La Commission recommande que les articles 18 et 64 du projet de loi nº 64 soient modifiés afin de prévoir que le recours à une technologie permettant d'identifier, de localiser ou d'effectuer le profilage d'une personne confère le droit de s'opposer à un tel recours et oblige à prévoir des mécanismes pour désactiver ces fonctions.**

RECOMMANDATION 4

La Commission recommande que le projet de loi nº 64 soit modifié afin de prévoir un droit à l'explication pour l'ensemble des décisions qui prennent appui sur un traitement automatisé des renseignements personnels.

RECOMMANDATION 5

La Commission recommande que les seuls cas où un organisme public ou une entreprise puisse utiliser un renseignement personnel à d'autres fins que celles pour lesquelles il ou elle l'a recueilli soient :

- **avec le consentement de la personne concernée;**
- **si l'utilisation est nécessaire à l'application d'une loi au Québec, après en avoir informé la Commission d'accès à l'information; ou**
- **sur autorisation de la Commission d'accès à l'information.**

RECOMMANDATION 6

La Commission recommande, le cas échéant, de préciser et circonscrire la notion de fins compatibles dans le respect des droits et libertés de la personne garantis par la Charte, notamment le droit au respect de sa vie privée.

RECOMMANDATION 7

La Commission recommande, le cas échéant, que les renseignements personnels sensibles ne puissent être utilisés à des fins compatibles sans le consentement de la personne concernée.

RECOMMANDATION 8

La Commission recommande que la notion « d'attente raisonnable de vie privée » soit retirée du projet de loi nº 64.

RECOMMANDATION 9

La Commission recommande que le projet de loi prévoie une définition plus précise de ce que constitue un renseignement sensible en tenant compte, entre autres, des motifs de discrimination prohibés par la Charte.

RECOMMANDATION 10

La Commission recommande que le projet de loi nº 64 soit modifié afin que la considération primordiale que constitue l'intérêt de l'enfant dans toute décision le concernant ainsi que le droit de l'enfant d'exprimer son opinion sur toute question l'intéressant et d'être entendu dans toute procédure judiciaire ou administrative l'intéressant soient reconnus dans la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels dans le secteur privé*.

RECOMMANDATION 11

La Commission recommande que le projet de loi nº 64 prévoie que les informations données à la personne mineure lors de l'obtention de son consentement soient adaptées à son âge et sa compréhension.

RECOMMANDATION 12

La Commission recommande que le projet de loi nº 64 prévoie que l'évaluation des impacts relatifs à la vie privée fasse l'objet d'une supervision externe par un tiers indépendant.

RECOMMANDATION 13

La Commission recommande que soit remplacée l'expression « facteurs relatifs à la vie privée » par celle de « facteurs relatifs aux droits et libertés de la personne garantis par la Charte », et ce, dans l'ensemble du projet de loi.

RECOMMANDATION 14

La Commission recommande que le projet de loi nº 64 réfère aux droits et libertés de la personne garantis par la Charte.

RECOMMANDATION 15

La Commission recommande que la notion d'anonymisation ne soit pas introduite au projet de loi nº 64.

RECOMMANDATION 16

La Commission recommande que l'alinéa 3 (2°) de l'article 28.1 de la *Loi sur la protection des renseignements personnels dans le secteur privé*, qui serait introduit par l'article 113 du projet de loi nº 64, soit remplacé par « du fait que la personne concernée était mineure au moment de la diffusion ».

RECOMMANDATION 17

La Commission recommande de modifier l'article 113 du projet de loi nº 64 qui introduirait l'article 28.1 al. 3.3 dans la *Loi sur la protection des renseignements personnels dans le secteur privé* pour clarifier qu'il vise à protéger les renseignements exacts, sans porter atteinte au droit de faire rectifier les renseignements inexacts.

RECOMMANDATION 18

La Commission recommande que le projet de loi nº 64 recoure à des infractions administratives ou à des infractions pénales plutôt qu'à des sanctions administratives pécuniaires.