Consultation sur les propositions du Commissariat à la protection de la vie privée du Canada visant à assurer une réglementation adéquate de l'intelligence artificielle

Observations présentées par la

Au Commissariat à la protection de la vie privée du Canada

L'intelligence artificielle : des lois inadéquates

Mars 2020

Présentation de la Ligue des droits et libertés

Fondée en 1963, la Ligue des droits et libertés (LDL) est un organisme à but non lucratif, indépendant et non partisan, qui vise à faire connaitre, à défendre et à promouvoir l'universalité, l'indivisibilité et l'interdépendance des droits reconnus dans la Charte internationale des droits de l'Homme. La Ligue des droits et libertés est affiliée à la Fédération internationale des ligues des droits humains (FIDH).

La LDL poursuit, comme elle l'a fait tout au long de son histoire, différentes luttes contre la discrimination et contre toute forme d'abus de pouvoir, pour la défense des droits civils, politiques, économiques, sociaux et culturels. Son action a influencé plusieurs politiques publiques et a contribué à la création d'institutions vouées à la défense et à la promotion des droits humains, notamment l'adoption de la Charte québécoise des droits et libertés de la personne du Québec et la création de la Commission des droits de la personne et des droits de la jeunesse.

Elle interpelle, tant sur les scènes nationale qu'internationale, les instances gouvernementales pour qu'elles adoptent des lois, mesures et politiques conformes à leurs engagements à l'égard des instruments internationaux de défense des droits humains et pour dénoncer des situations de violation de droits dont elles sont responsables. Elle mène des activités d'information, de formation, de sensibilisation visant à faire connaitre le plus largement possible les enjeux de droits pouvant se rapporter à l'ensemble des aspects de la vie en société. Ces actions visent l'ensemble de la population de même que certains groupes placés, selon différents contextes, en situation de discrimination.

Nous remercions le Commissariat à la protection de la vie privée (Commissariat) de cette invitation à participer à la *Consultation sur les propositions du Commissariat visant à assurer une réglementation adéquate de l'intelligence artificielle*[1].

L'objet de la consultation du Commissariat

Rappelons l'objet de cette consultation :

> Nous (Le Commissariat) examinons l'intelligence artificielle (IA) dans le contexte de ces travaux en lien en particulier avec la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Nous sommes d'avis que la LPRPDE est inadéquate en ce qui concerne son application aux systèmes d'IA et nous avons relevé plusieurs domaines dans lesquels la LPRPDE pourrait être renforcée .

Le Commissariat désire donc :

> […] valider sa compréhension de la façon dont les principes de protection de la vie privée devraient s'appliquer à l'élaboration et au déploiement des systèmes d'IA et déterminer si ses propositions sont compatibles avec la conception et le déploiement responsables de ces systèmes.

Mise en contexte - Des lois inadéquates

À l'instar du Commissariat, nous estimons que les lois de protection des renseignements personnels (fédérales ou provinciales) adoptées dans les années '80 et '90 sont totalement inadéquates à l'ère de l'internet et particulièrement dans le contexte du développement effréné de l'intelligence artificielle (incluant l'apprentissage machine, l'apprentissage profond et le *Big data*). Le siphonnage massif de données sur les réseaux sociaux, la reconnaissance faciale, l'internet des objets, les systèmes de localisation GPS, les drones dopés à l'IA, les capteurs de données des villes intelligentes, les assistants vocaux aux noms rassurants : tout cet attirail d'encerclement se développe sans contrôle ni débat public et parait en voie d'anéantir toute possibilité de vie privée, en plus de mettre à mal de nombreux autres droits humains. Comme le souligne l'auteur Nick Srnicek, « la suppression de la vie privée appartient à l'essence même des plateformes, qui exercent une pression constante contre les limites de ce qui est socialement acceptable en termes de collecte de données »[2].

---

[1] *Consultation sur les propositions du Commissariat visant à assurer une réglementation adéquate de l'intelligence artificielle*, https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultation-ai/pos_ai_202001/

[2] Srnicek, Nick, *Capitalisme de plateforme : l'hégémonie de l'économie numérique*, Lux éditeurs, 2018, P.106.

La reconnaissance faciale offre un bel exemple des risques que présente le développement incontrôlé et chaotique de systèmes basés sur l'IA. Certains corps policiers utilisent ou auraient déjà utilisé cette technologie au pays[3], tandis que d'autres refusent de dire s'ils en font usage[4]. Les photos utilisées pour mettre au point l'une de ces applications proviendraient des réseaux sociaux[5]. La reconnaissance faciale servirait aussi dans certains centres commerciaux à des fins de marketing[6]. La commercialisation de cette technologie pourrait s'étendre bientôt à d'autres secteurs[7].

Il est à souligner que cette technologie de reconnaissance des individus n'est pas que « faciale », elle s'intéresse autant à l'allure, au comportement ou à l'habillement des personnes surveillées. Les individus ne sont pas tant ciblés pour « ce qu'ils font » que pour « ce qu'ils sont ». Cette surveillance est d'autant plus inquiétante alors que certains groupes racisés sont victimes de discrimination systémique de la part des forces policières. Les auteur-e-s d'un rapport de 2019 sur les interpellations policières à Montréal écrivaient :

> Aussi, il faut tenir compte du fait que **le profilage criminel, fondé sur la prédiction, s'appuie sur des éléments liés directement ou indirectement à l'appartenance « raciale »** (la couleur de peau, certes, mais également l'habillement, la démarche, la gestuelle corporelle ou tout simplement le lieu de résidence), ce qui peut avoir pour effet d'accentuer les disparités raciales existantes. C'est pourquoi il est nécessaire de dévoiler et de comprendre les forces structurelles et systémiques qui encouragent la production de discriminations raciales[8].

Ces outils de surveillance battent en brèche le droit à la vie privée et à l'anonymat, tout en rendant possible le profilage discriminatoire. Ils semblent pourtant se développer sans aucun contrôle, malgré qu'existent au Québec certaines balises légales[9], de toute évidence, inefficaces ou non respectées.

---

[3] Gagnon, Charles-Antoine, « Le SPO a déjà expérimenté un outil de reconnaissance faciale », *Le Droit*, 24 février 2020, https://www.ledroit.com/actualites/justice-et-faits-divers/le-spo-a-deja-experimente-un-outil-de-reconnaissance-faciale-c42e84e649af176165e20eb536123117

[4] Péloquin, Tristan, « Reconnaissance faciale: le SPVM refuse de dire s'il utilise un logiciel controversé », *La Presse*, 18 février 2020, https://www.lapresse.ca/actualites/grand-montreal/202002/17/01-5261371-reconnaissance-faciale-le-spvm-refuse-de-dire-sil-utilise-un-logiciel-controverse.php

[5] « Google, Facebook et Twitter mettent en demeure Clearview AI », *Radio-Canada*, 6 février 2020, https://ici.radio-canada.ca/nouvelle/1509484/clearview-ai-intelligence-artificielle-reconnaissance-faciale

[6] Couture, Pierre, « Reconnaissance faciale : les consommateurs épiés à leur insu dans les commerces », *Journal de Québec,* 11 mai 2019, https://www.journaldequebec.com/2019/05/11/souriez-on-vous-surveille-par-la-reconnaissance-faciale

[7] Malboeuf, Marie-Claude, « Bell veut vous suivre en continu », *La Presse*, 26 février 2020, https://www.lapresse.ca/actualites/202002/26/01-5262536-bell-veut-vous-faire-suivre-en-continu.php Malboeuf, Marie-Claude et Lévesque, Fanny, « Reconnaissance faciale: indignation et inquiétude à Québec et à Ottawa », *La Presse*, 28 février 2020, https://www.lapresse.ca/actualites/politique/202002/27/01-5262688-reconnaissance-faciale-indignation-et-inquietude-a-quebec-et-a-ottawa.php

[8] Armony, Victor et al., *Les interpellations policières à la lumière des identités racisées, Analyse des données du Service de Police de la Ville de Montréal (SPVM) et élaboration d'indicateurs de suivi en matière de profilage racial, Rapport final remis au SPVM,* août 2019, p. 8.

[9] L'article 45 de la *Loi concernant le cadre juridique des technologies de l'information* (L.R.Q. c. C-1.1) prévoit : « La création d'une banque de caractéristiques ou de mesures biométriques doit être préalablement divulguée à la Commission d'accès à l'information. De même, doit être divulguée l'existence d'une telle banque qu'elle soit ou ne soit pas en service. La Commission peut rendre toute ordonnance concernant de telles banques afin d'en déterminer la confection, l'utilisation, la consultation, la communication et la conservation y compris l'archivage ou la destruction des

Le Commissariat et les commissaires de quelques provinces viennent de lancer une enquête sur la reconnaissance faciale, ce que nous saluons. Mais ce dossier illustre le peu de moyens dont disposent les commissions de protection des renseignements personnels qui, trop souvent, n'interviennent qu'après coup alors que l'usage de telles technologies devrait plutôt être strictement interdit, sauf autorisation judiciaire.

Cela dit, les enjeux entourant l'IA vont bien au-delà de la question de la vie privée. L'érosion des logiques collectives est aussi en cause. L'enfermement algorithmique mine le droit à l'information et la capacité de mener des débats publics éclairés. La « quantification de soi » et autres capteurs de données personnelles peuvent remettre en cause les principes de mutualisation (en assurances notamment) et de solidarité sociale. La surveillance de masse porte aussi atteinte à la vie démocratique.

Nous sommes d'avis que ces enjeux doivent faire l'objet de débats publics en posant les questions suivantes :

- Qui peut utiliser l'IA?
- À quelles fins?
- Dans quelles conditions?
- Quelles garanties s'imposent en termes de publicité, de reddition de comptes et de responsabilité dans l'usage de ces algorithmes et technologies impliquant l'IA?

Par ailleurs il appartient à l'État, au terme de ces débats, de fixer les limites et de définir les responsabilités assurant une protection véritable de la vie privée et des autres droits fondamentaux.

Observations sur les propositions du Commissariat

Proposition 1 : Incorporer dans la loi une définition de l'IA qui servirait à distinguer les règles juridiques qui ne s'appliqueraient qu'à elle, tandis que les autres règles s'appliqueraient à tout type de traitement, y compris l'IA

Comme l'indique le Commissariat : « La LPRPDE est neutre sur le plan technologique et constitue une loi d'application générale. À ce titre, elle ne comprend pas de définition relative à l'IA, à la prise de décision automatisée ou au traitement automatisé. Toutefois, tel que nous le suggérons dans certaines autres propositions de ce document, il pourrait être nécessaire d'établir des règles

mesures ou caractéristiques prises pour établir l'identité d'une personne. La Commission peut aussi suspendre ou interdire la mise en service d'une telle banque ou en ordonner la destruction, si celle-ci ne respecte pas ses ordonnances ou si elle porte autrement atteinte au respect de la vie privée ».

particulières pour certaines utilisations de l'IA, ce qui justifierait de la définir dans la loi pour préciser quand ces règles s'appliqueraient. »

La LDL souscrit au principe de neutralité technologique selon lequel les lois doivent s'appliquer sans égard aux moyens technologiques par lesquels s'accomplissent les activités visées. Les lois de protection des renseignements personnels s'étendent à l'internet, même si elles sont, de fait, souvent non respectées. Le manque de pouvoirs du Commissaire en vertu de la LPRPDE explique en partie ce fait.

Si le caractère général de la LPRPDE doit être maintenu, le Commissariat doit pouvoir édicter des lignes directrices contraignantes pour préciser l'application de la loi à un domaine si vaste et complexe que l'IA.

Nous ne nous prononçons pas sur la définition de l'IA qu'il convient d'inscrire dans la loi. Celle-ci devrait cependant être la plus large possible.

Proposition 2 : Adopter une approche fondée sur les droits dans la loi, selon laquelle les principes de protection des données sont mis en œuvre comme moyen de protéger un droit plus général à la vie privée – reconnu comme un droit fondamental de la personne et comme fondement de l'exercice d'autres droits de la personne

Nous souscrivons à l'approche fondée sur les droits.

La Cour suprême distingue trois facettes à la vie privée : l'aspect spatial ou territorial; l'aspect relatif à la personne et enfin le volet informationnel qui concerne « le droit du particulier de déterminer lui-même quand, comment et dans quelle mesure il diffusera des renseignements personnels le concernant »[10].

L'IA a un impact sur toutes les facettes de la vie privée. En plus de mettre en jeu la protection et l'utilisation de renseignements personnels, l'IA peut interférer avec le volet spatial (par exemple par géolocalisation) et le volet lié à la personne (atteinte à l'intimité, à l'autonomie).

Cette technologie compromet aussi les autres droits humains. Notamment, elle rend possible une surveillance extrême des individus (tant par des entreprises privées que par l'État) susceptible d'affecter la liberté d'expression, la liberté d'association et la démocratie[11]. La reconnaissance faciale met en péril le droit à l'anonymat et éventuellement le droit à l'égalité[12]. Les chambres d'écho des réseaux sociaux peuvent, quant à elles, amoindrir la circulation de l'information et la

[10] R. c. Dyment, 1988 CanLII 10 (CSC), [1988] 2 RCS 417. https://www.canlii.org/fr/ca/csc/doc/1988/1988canlii10/1988canlii10.html?searchUrlHash=AAAAAQAVZHItZW50IGIuZm9ybWF0aW9ubmVsAAAAAAE&resultIndex=1

[11] R. c. Mills, 2019 CSC 22 : « De nombreuses études empiriques ont confirmé l'« effet paralysant » de la surveillance gouvernementale sur les comportements en ligne. Ces études indiquent que la surveillance électronique par l'État incite les gens à exercer l'autocensure sur leur expression en ligne », https://www.canlii.org/fr/ca/csc/doc/2019/2019csc22/2019csc22.html?searchUrlHash=AAAAAQARbWlsbHMgYXV0b2NlbnN1cmUAAAAAAQ&resultIndex=1

[12] Armony, Victor et al, *Les interpellations policières à la lumière des identités racisées*, *op cit*. note 9.

diversité d'opinions et mener à de la manipulation commerciale ou politique. En outre, des algorithmes mal calibrés peuvent entretenir - voire aggraver - des pratiques discriminatoires[13].

Bref, la cueillette, l'utilisation et le traitement de données personnelles par l'IA dépassent de loin la seule question de la protection des données, cela concerne la vie privée au sens large, de même que l'ensemble des autres droits fondamentaux. La LPRPDE devrait être modifiée pour refléter ce fait.

Proposition 3 : La loi devrait prévoir le droit de s'opposer à la prise de décision automatisée et de ne pas être soumis à des décisions fondées uniquement sur un traitement automatisé, sous réserve de certaines exceptions

Nous sommes d'accord avec l'introduction d'un droit d'opposition à la prise de décision automatisée. Ce droit devrait pouvoir s'exercer à toutes les étapes du processus. Par ailleurs, même s'il y a consenti, l'individu devrait avoir accès aux critères ayant conduit à la décision et aussi, pouvoir en contester le bien-fondé.

La loi devrait aussi reconnaitre un droit d'opposition similaire à celui de l'art. 21 du *Règlement Général sur la Protection des Données* (RGPD)[14]. La personne concernée doit pouvoir s'opposer à tout moment au traitement de ses données. Et cela, même si ce traitement est nécessaire à l'exécution d'une mission d'intérêt public ou nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers. Seules exceptions : le responsable du traitement démontre qu'il existe des motifs légitimes et impérieux pour le traitement, qui prévalent sur les intérêts et les droits et libertés de la personne concernée; ou encore si le traitement est nécessaire pour la constatation, l'exercice ou la défense de droits en justice.

Le traitement de données à des fins de prospection directe (marketing) devrait être interdit sauf consentement exprès.

Proposition 4 : Donner aux personnes le droit à une explication et à une plus grande transparence lorsqu'elles interagissent avec un traitement automatisé ou font l'objet d'un tel traitement

Le respect de la transparence est essentiel. Nous estimons que ce principe doit faire l'objet d'une approche collective. Le fonctionnement logique des algorithmes devrait être divulgué

---

[13] Paré, Isabelle, « La main invisible des algorithmes », *Le Devoir,* 8 février 2017, https://www.ledevoir.com/societe/science/492029/le-pouvoir-des-codes-la-main-invisible-des-algorithmes

[14] La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur l'article 6, paragraphe 1, point e) ou f), y compris un profilage fondé sur ces dispositions. Le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice. (article 21 (1) RGPD)

publiquement et de façon proactive; c'est ce que la Commission nationale de l'informatique et des libertés (CNIL) inclut dans le principe de loyauté :

> […] alors que dans la loi Informatique et Libertés, l'information est un droit qui peut éventuellement être mobilisé par l'individu auprès du responsable de l'algorithme, avec le principe de loyauté, cette information doit d'emblée être diffusée à destination de la communauté des utilisateurs. Il n'est pas question ici de droit des utilisateurs, mais d'obligation des plateformes algorithmiques. Dans cette mesure, la loyauté semble à même de constituer une réponse au problème de l'asymétrie entre les responsables des algorithmes et les utilisateurs[15].

L'obligation de divulgation proactive devrait même s'appliquer aux algorithmes n'utilisant pas de renseignements personnels « dans la mesure où ceux-ci sont susceptibles d'avoir des impacts collectifs significatifs »[16].

Un système d'audit indépendant pourrait garantir que les algorithmes utilisés respectent la loi et sont exempts de biais discriminatoires[17].

Cela dit, il va de soi qu'un individu touché par le traitement automatisé de ses données doit pouvoir comprendre comment une décision le concernant a été prise. Tout comme il devrait bénéficier d'un droit de contestation de cette décision.

Proposition 5 : Exiger l'application des principes de la protection de la vie privée dès la conception et des droits de la personne dès la conception à toutes les étapes du traitement, y compris la collecte de données

Le *privacy by design* (et *by default*) devrait s'appliquer à toutes les étapes du traitement de données. Les sept principes[18] de ce concept devraient constituer une norme légale.

Quant au respect des « droits-humains-*by-design* », il suppose que des évaluations d'impacts des algorithmes sur les droits fondamentaux soient effectuées avant leur déploiement et tout au long de leur utilisation. Cela nous apparait indispensable, les biais discriminatoires des algorithmes étant reconnus.

---

[15] Commission nationale de l'informatique et des libertés, *Comment permettre à l'Homme de garder la main? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, décembre 2017, p.50, https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf

[16] *Op cit,* p.56.

[17] Commission nationale de l'informatique et des libertés, « Développer l'audit des algorithmes de manière à contrôler leur conformité à la loi et leur loyauté est une solution fréquemment évoquée pour assurer leur loyauté, leur responsabilité et, plus largement, leur conformité à la loi », *op. cit,* p.57.

[18] Des mesures proactives et préventives; Une protection implicite et automatique; Une intégration de la vie privée dans la conception des systèmes et au cœur des pratiques; Une protection intégrale; Une sécurité de bout en bout, durant toute la durée de la conservation des données; Assurer la visibilité et la transparence; Respecter la vie privée des utilisateurs (en privilégiant les intérêts des particuliers). Voir *Commission nationale pour la protection des données,* 24 juillet 2017, https://cnpd.public.lu/fr/dossiers-thematiques/nouvelles-tech-communication/privacy-by-design/Le-Privacy-by-Design_-de-quoi-s_agit-il_.html

De nombreux cas[19] démontrent en effet que des vices de conception ou l'utilisation de données historiques biaisées peuvent conduire l'algorithme à reproduire, voire aggraver, des attitudes et comportements discriminatoires. Selon *AccesNow*, ces biais seraient la règle plutôt que l'exception[20].

L'utilisation de l'IA dans l'analyse de données se généralise à tous les secteurs. Les algorithmes peuvent intervenir dans le recrutement en emploi, l'établissement de cotes de crédit financières, l'accès à des établissements d'enseignement, l'évaluation des demandes d'immigration et de statut de réfugié-e-s[21], dans le système de justice[22], la détection de la fraude, le droit à certains services ou prestations, etc. Son utilisation est susceptible d'affecter de façon disproportionnée les groupes déjà discriminés socialement. Il convient donc de s'assurer qu'un algorithme ne reproduise pas des attitudes et comportements discriminatoires en raison d'un vice de construction ou par utilisation de données historiquement biaisées.

Proposition 6 : Faire en sorte que le respect des principes de la finalité et de la minimisation des données dans le contexte de l'IA soit à la fois réaliste et efficace

L'industrie prétend avoir besoin de toujours plus de données pour alimenter l'IA; la vie privée devrait céder le pas en conséquence. Nous n'adhérons pas, bien sûr, à cette vision.

Les traces numériques que nous laissons derrière nous se multiplient et mettent en péril le concept même de vie privée, comme le souligne *Accesnow* :

> The risks due to ability of AI to track and analyze our digital lives are compounded because of the sheer amount of data we produce today as we use the internet. With the increased use of Internet of Things (IoT) devices and the attempts to shift toward "smart cities," people will soon be creating a trail of data for nearly every aspect of their lives. Although the individual pieces of this data may seem innocuous, when aggregated they reveal minute details about our lives. AI will be used to process and analyze all this data for everything from micro-targeted advertising, to optimizing public transportation, to government surveillance of citizens. In such a world, not only are there huge risks to privacy, but the situation raises the question of whether data protection will even be possible[23].

---

[19] Collard, Nathalie, « Nos robots seront-ils machos? », *La Presse*, 29 mai 2019, https://www.lapresse.ca/societe/201905/29/01-5227959-nos-robots-seront-ils-machos-.php

[20] « Unfortunately, biased data and biased parameters are the rule rather than the exception. Because data are produced by humans, the information carries all the natural human bias within it. », Access Now, *Human rights in the age of artificial intelligence,* nov.2018, p.12, https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf

[21] Kenyon, Miles, " Bots at the gate ", *The Citizenlab*, 26 septembre 2018, https://citizenlab.ca/2018/09/bots-at-the-gate-human-rights-analysis-automated-decision-making-in-canadas-immigration-refugee-system/

[22] Cyr, Hugo et al., « Pour un développement éthique et responsable de l'IA en droit », *Le Devoir,* 8 décembre 2018, https://www.ledevoir.com/societe/science/542970/pour-un-developpement-ethique-et-responsable-de-l-ia-en-droit

[23] *Op cit.,* note 14, p. 21

Le professeur de droit à l'Université du Maryland, Frank Pasquale, note quant à lui :

> À mesure que les capteurs des téléphones portables s'améliorent, les Géants du Web sont toujours davantage tentés de collecter encore plus de données, jusqu'à obtenir un portrait complet des utilisateurs, qui met à nu leurs vulnérabilités, leurs désirs, leurs faiblesses, voire leurs crimes[24].

Cette industrie insatiable a pour finalité l'espionnage à grande échelle de la population. Comme l'explique la professeure Zuboff, de la *Harvard Business School*, le modèle d'affaires consiste dans l'extraction et la vente de la vie privée des usagers et usagères à d'autres entreprises, sous la forme de modèles prédictifs[25]. Une telle surveillance (finalité) devrait être interdite, selon nous. Elle suppose une renonciation générale - et à l'avance - à la vie privée des utilisateurs et utilisatrices des réseaux sociaux. Il devient pratiquement impossible de connaitre avec exactitude l'ampleur de la renonciation. Frank Pasquale note : « Quand les citoyens exigent que Facebook et Google leur transmettent leur dossier personnel, ils découvrent avec horreur que de vastes réserves de vidéos, de conversations intimes et de photographies qu'ils pensaient avoir supprimés sont parfaitement préservés dans des archives. Des enregistrements détaillés de leurs déplacements émergent[26] ».

Le consentement apparaît aussi vicié du fait qu'il n'est pas négociable : c'est à prendre ou à laisser. Or, l'accès aux réseaux sociaux et autres plateformes sur internet est pratiquement essentiel de nos jours. La Cour suprême notait en 2017 :

> Comme le souligne l'intervenante Association canadienne des libertés civiles, [traduction] « l'accès à Facebook et aux plateformes de média social, y compris les communautés en ligne qu'ils rendent possibles, a vu son importance s'accroître dans l'exercice de la liberté d'expression et de la liberté d'association, ainsi que dans la pleine participation à la démocratie » (mémoire de l'Association canadienne des libertés civiles, par. 16). Le choix de « ne pas être en ligne » ne saurait constituer un choix véritable à l'ère d'Internet[27].

La LDL ne croit donc pas qu'il faille renoncer aux garde-fous, même fragiles, de la finalité et de la cueillette minimale de données. Au contraire, l'État devrait garantir le droit à la vie privée par défaut et interdire le consentement du type « tout-ou-rien » en laissant la possibilité aux individus de choisir facilement et clairement les informations dont ils acceptent la collecte.

---

[24] Pasquale, Frank, « Mettre fin au trafic des données personnelles », *Le Monde diplomatique.* Mai 2018, p. 16-17.
[25] « Nous sommes les objets dont la matière est extraite, expropriée, puis injectée dans les usines d'intelligence artificielle de GOOGLE qui fabriquent les produits prédictifs vendus aux clients réels :les entreprises qui paient pour jouer sur les nouveaux marchés comportementaux. »
Zuboff, Shoshana, « Un capitalisme de surveillance », *Le Monde diplomatique,* janvier 2019, pp.10-11
[26] Pasquale, Frank*, op.cit,* note 17.
[27] Douez c. Facebook, Inc., 2017 CSC 33
https://www.canlii.org/fr/ca/csc/doc/2017/2017csc33/2017csc33.html?searchUrlHash=AAAAAQAOZG91ZXogaW50ZXJuZXQAAAAAAQ&resultIndex=1

Proposition 7 : Inclure dans la loi d'autres motifs de traitement et des solutions pour protéger la vie privée lorsqu'il n'est pas possible d'obtenir un consentement valable

Le modèle législatif basé sur le consentement fait actuellement l'objet de nombreuses récriminations. Il serait inefficace et engendrerait un faux sentiment de sécurité.

Ces critiques sont largement fondées. Le consentement se trouve souvent vicié, notamment par ignorance de l'étendue réelle de la collecte ou de l'utilisation qui seront faites des données. Ce consentement est de plus souvent « extorqué » dans la mesure où le choix n'existe pas; c'est tout ou rien. Par ailleurs, les entreprises l'obtiennent sur un simple clic, censé prouver l'acceptation de longues politiques d'utilisation souvent indéchiffrables.

Mais laisser tomber totalement le modèle du consentement signifierait que l'individu n'a plus voix au chapitre sur l'information le concernant. Cela parait aberrant. Il faut revoir le modèle, mais non s'en défaire totalement. Il importe que l'individu puisse invoquer l'absence de consentement. Cependant, le consentement de l'usager ou de l'usagère ne doit pas dégager l'entreprise de toute responsabilité, par exemple, lorsque les données récoltées sont excessives, sans lien avec la finalité ou que la personne n'avait pas le choix de consentir.

Le consentement individuel ne constitue toutefois pas la panacée. Il ne saurait suffire dans un monde où l'utilisation des données engendre des conséquences importantes au plan collectif. Ainsi, le consentement peut impliquer le dévoilement de la vie privée de tiers. Comme le note à juste titre l'auteur Philippe de Grosbois :

> […] lorsqu'une personne détient une adresse Gmail et qu'elle a donc « consenti » à ce que tous ses courriels soient entreposés de manière permanente sur les serveurs de Google, cela signifie que toutes les personnes à qui elle a écrit et qui lui ont écrit sont aussi partiellement l'objet de ce stockage de données. C'est en envisageant la protection de la vie privée comme un enjeu collectif plutôt que comme le fruit d'ententes individuelles qu'il sera véritablement possible d'avancer[28].

Les enjeux collectifs entourant le traitement de données massives commandent l'édiction d'obligations légales de transparence et d'explication des modes de fonctionnement des systèmes. Le professeur Pierre Trudel note à cet égard :

> Hormis des obligations de surmultiplier les mentions et « conditions d'utilisation », les lois n'imposent pratiquement pas d'exigences de transparence et de reddition de comptes quant à la façon dont les entreprises génèrent de la valeur avec les données de tout un chacun. (…) Alourdir les obligations d'obtenir les consentements individuels sans augmenter les exigences de responsabilisation à l'égard des processus de décision des entreprises, c'est passer à côté des véritables enjeux[29].

---

[28] de Grosbois, Philippe, *Les batailles d'internet : assauts et résistances à l'ère du capitalisme numérique,* Les Éditions Écosociété, 2018, p.156

[29] Trudel, Pierre, « Renseignements personnels : les vraies urgences », *Le Devoir,* 18 février 2020, p. A 7, https://www.ledevoir.com/opinion/chroniques/573151/renseignements-personnels-les-vraies-urgences

Proposition 8 : Établir des règles qui permettent une certaine souplesse dans l'utilisation des renseignements qui ont été rendus non identifiables, tout en s'assurant qu'il existe des mesures plus rigoureuses pour assurer une protection contre la réidentification

Le document de consultation du Commissariat souligne que: « De nombreux pays considèrent les données désidentifiées ou rendues anonymes comme des renseignements non personnels hors du champ d'application de la loi. »

À l'instar du Commissariat, nous rejetons ce point de vue. L'anonymisation n'est pas une technique sans failles. Les risques de réidentification sont bien réels[30]. Les lois de protection des données doivent donc s'appliquer.

L'utilisation de renseignements anonymisés à des fins de recherches, utiles socialement, pourrait éventuellement constituer une exception valable à la nécessité du consentement. Une telle utilisation devrait toutefois être autorisée par l'organisme de réglementation et respecter les conditions prescrites.

Proposition 9 : Exiger des organisations qu'elles assurent la traçabilité des données et des algorithmes, notamment en ce qui concerne les ensembles de données, les processus et les décisions prises pendant le cycle de vie du système d'IA

Pour les raisons mentionnées précédemment, notamment aux points 4 (transparence), 5 (respect-des-droits-humains-*by-design*) et 7 (consentement), il est essentiel de pouvoir retracer, analyser et valider les résultats d'un système d'IA. Il convient en outre que la conformité du système (respect des droits humains, de la vie privée et autres obligations légales) puisse faire l'objet d'un contrôle.

Une thèse veut que les algorithmes utilisés en apprentissage automatique (*machine learning*) génèreraient des décisions indéchiffrables[31] . Ce n'est pas un argument défendable pour la LDL. Dans la mesure où des décisions affectant les personnes sont prises sur la base de ces algorithmes, il est essentiel que les raisonnements sous-jacents soient compréhensibles, que les responsabilités soient clairement définies et qu'un droit de recours existe.[32] Autrement dit : « Si des entreprises prétendent que leurs algorithmes sont trop complexes pour être révélés, les autorités devraient interdire l'utilisation des informations qui en résultent »[33].

---

[30] Gravel, Pauline, « Données personnelles: un secret mal gardé », *Le Devoir,* 26 juillet 2019, https://www.ledevoir.com/societe/science/559444/un-secret-mal-garde

[31] « Because they identify so many patterns, they are too complex for humans to understand, and thus it is not possible to trace the decisions or recommendations they make. In addition, many machine learning algorithms constantly re-calibrate themselves through feedback .», Accesnow, *op.cit*, note 14. p.13.

[32] Commissaire aux droits de l'homme , Conseil de l'Europe, « Protéger les droits de l'homme à l'ère de l'intelligence artificielle », 7 mars 2018, https://www.coe.int/fr/web/commissioner/-/safeguarding-human-rights-in-the-era-of-artificial-intelligence

[33] Pasquale, Frank*, op.cit,* note 17.

Par ailleurs, il appartient à l'État[34] de mettre en place les mesures de contrôles garantissant que les systèmes d'IA utilisés tant dans le secteur privé que public respectent les droits humains et la vie privée :

> On ne devrait pas attendre des seuls individus la mise en exergue des problèmes liés aux données de masse et aux processus de décision automatisés. Les particuliers n'ont pas le temps d'explorer les milliers de bases qui pourraient avoir un impact sur leur vie. La détection des failles dans leur exploitation incombe aux autorités, qui doivent examiner les inventaires des serveurs des grandes entreprises et des courtiers afin de trouver les données suspectes et exiger une traçabilité pour vérifier la fiabilité de leurs sources [...] Il suffirait de taxer un peu l'économie des données pour financer des contrôles plus larges. [35].

Proposition 10 : Obliger à faire preuve de responsabilité démontrable pour l'élaboration et la mise en œuvre du traitement par IA

Proposition 11 : Donner au Commissariat le pouvoir d'émettre des ordonnances exécutoires et d'imposer des sanctions financières aux organisations qui ne se conforment pas à la loi

Selon le document de consultation, la responsabilité démontrable « exigerait des organisations qu'elles soient en mesure de prouver, sur demande, qu'elles se conforment aux exigences de la loi ». Des pouvoirs d'inspections proactives, semblables à ceux prévus à la *Loi sur la protection des renseignements personnels* (loi visant le secteur public), seraient attribués au Commissariat. La vérification indépendante des systèmes d'IA serait obligatoire et le Commissariat aurait le pouvoir d'imposer des sanctions financières en cas de non-conformité à la loi. C'est ce que réclame le Commissariat.

Il apparait que cet « arsenal » de moyens plutôt modestes aurait dû faire partie intégrante de la LPRPDE dès son adoption. La faiblesse des pouvoirs du Commissariat est navrante et mine sérieusement l'application de la loi.

Le dossier *Facebook-Cambridge Analytica* le démontre amplement. Le géant du Web refuse de donner suite aux recommandations du Commissariat visant à remédier à de graves lacunes en matière de vie privée. En conséquence, le Commissariat doit recommencer le processus devant la

---

[34] *Déclaration de Toronto sur l'intelligence artificielle*, mai 2018,
« 24. Les États ont l'obligation positive de protéger la population contre les discriminations pratiquées par les acteurs du secteur privé et de promouvoir l'égalité et les autres droits fondamentaux, notamment en adoptant des lois contraignantes. », « Article 26. Les États doivent s'assurer que les mesures existantes visant à prévenir la discrimination et d'autres atteintes aux droits humains soient mises à jour de manière à prendre en compte les risques posés par les technologies reposant sur l'apprentissage automatique et à y remédier. »,
https://www.torontodeclaration.org/declaration-text/francais/

[35] *Op. cit, Déclaration de Toronto sur l'intelligence artificielle*.

Cour fédérale[36]. Pendant ce temps, les renseignements personnels de milliers d'usagers canadiens et d'usagères canadiennes demeurent à risque.

Bien des entreprises ne prendront les moyens nécessaires afin de respecter le cadre législatif canadien que lorsqu'elles y seront contraintes par de fortes amendes[37], des sanctions pénales et des pouvoirs d'ordonnance. Cela vaut d'ailleurs tout autant pour l'État. Les fuites de renseignements personnels s'accumulent, tant du côté des entreprises[38] que des gouvernements,[39] sans que les mesures drastiques qui s'imposent ne soient prises pour corriger la situation.

Nous souscrivons à la proposition de faire du Commissariat à la vie privée l'instance de premier niveau pour entendre les plaintes des individus, rendre des ordonnances exécutoires et imposer des sanctions financières en cas de non-respect de la loi. Toutefois, ces mesures ne seront effectives que si le Commissariat dispose des ressources humaines et financières nécessaires à leur mise en application.

Sur le plan de la responsabilité civile, il va de soi que la faute pour les défaillances de conception des systèmes d'IA doit reposer sur les humains et les entreprises et non sur la machine. Il conviendrait de prévoir la **responsabilité solidaire** des différents intervenants dans la conception et la mise en œuvre d'un système d'IA, de même que des **présomptions de responsabilité**.

Dans un autre ordre d'idée, le gouvernement fédéral devrait se doter de mécanismes de consultation de la société civile concernant le développement et l'utilisation de l'intelligence artificielle.

Finalement, l'IA soulève des enjeux qui dépassent largement la portée de la LPRPDE, notamment des problèmes relatifs au droit d'auteur et au droit à l'information. Qui plus est, les géants du Web rachètent de plus en plus de *start-up*, acquérant du coup les données personnelles de leurs usagers et usagères : en 2016, *Microsoft* acquiert *LinkedIn*, héritant de ce fait des historiques d'emploi de millions de travailleurs et travailleuses[40]. *Google* vient de se porter acquéreur de *Fitbit,* qui possède de nombreuses données personnelles liées à la santé, la nutrition et la pratique sportive des utilisateurs et utilisatrices[41]. La concentration effarante de données personnelles

---

[36] Radio-Canada, « Facebook : le commissaire à la protection de la vie privée saisit la Cour fédérale », 6 février 2020, https://ici.radio-canada.ca/nouvelle/1509712/informations-personnelles-facebook-cour-federale

[37] Une amende de 5 milliards de dollars a été imposée à Facebook par la Commission fédérale du commerce des États-Unis dans le cadre du scandale Cambridge Analytica, voir *Agence France-Presse* et *Radio-Canada,* « Facebook payera une amende record de 5 milliards de dollars, selon des médias », 12 juillet 2019 », https://ici.radio-canada.ca/nouvelle/1221511/facebook-amende-record-5-milliards et *Agence France-Presse* et *Le Devoir,* Données privées: amende record de 5 milliards $US pour Facebook, 24 juillet 2019, https://www.ledevoir.com/monde/etats-unis/559321/donnees-privees-amende-record-de-5-milliards-de-dollars-pour-facebook

[38] Desjardins, Capital One, Industrielle Alliance, Trans Union, Equifax, Facebook-Cambridge-Analytica,Ashley Madison.

[39] Revenu Québec, ministère de l'Éducation du Québec, Agence du revenu du Canada, Postes Canada, Centre de la sécurité des télécommunications, ministère des Anciens Combattants, voir Duchaine, Hugo, « Données personnelles : des fuites qui se multiplient », *Journal de Montréal,* 12 février 2020, https://www.journaldemontreal.com/2020/02/12/donnees-personnelles-des-fuites-qui-se-multiplient

[40] Srnicek, Nick*, op.cit* note 2, p.114

[41] Chartier, Mathieu, « Google : les régulateurs européens inquiets au sujet des données Fitbit récupérées lors du rachat », *Les numériques,* 24 février 2020, https://www.lesnumeriques.com/montre-connectee/google-les-regulateurs-europeens-inquiets-au-sujet-des-donnees-fitbit-recuperees-lors-du-rachat-n147515.html

entre les mains de quelques joueurs devrait faire l'objet d'un examen sous l'angle des lois antitrust[42].

Comme le recommandait récemment le rapport Yale :

> L'examen des répercussions de l'utilisation de mégadonnées commande une approche multidimensionnelle et globale afin d'assurer l'élaboration de cadres législatifs et réglementaires exhaustifs. L'ensemble des autorités réglementaires sont concernées et doivent rapidement agir de concert. Au minimum Statistique Canada, le CRTC, le Commissariat à la protection de la vie privée et le Bureau de la concurrence devraient agir afin de développer un cadre de réglementation holistique capable de rendre compte des multiples dimensions associées à l'activité des entreprises impliquées dans l'usage et la valorisation des mégadonnées[43].

[42] Le comité judiciaire de la Chambre des représentants américaine a entrepris une enquête à ce sujet. Voir Krol, Ariane, « GAFA : Des géants trop gros pour notre bien? », *La Presse,* 16 septembre 2019, https://www.lapresse.ca/debats/editoriaux/201909/15/01-5241372-gafa-des-geants-trop-gros-pour-notre-bien-.php

[43] Groupe d'examen du cadre législatif en matière de radiodiffusion et de télécommunications, « L'avenir des communications au Canada : le temps d'agir », janvier 2020. p.211