Commission
d'accès à l'information
du Québec

Mémoire de la Commission d'accès à l'information

Pour un développement responsable de l'intelligence artificielle qui respecte le droit à la vie privée et responsabilise tous les acteurs impliqués

Présenté à la Déclaration de Montréal pour une intelligence artificielle responsable

Montréal, 29 mars 2018

Pour un développement responsable de l'intelligence artificielle qui respecte le droit à la vie privée et responsabilise tous les acteurs impliqués

Mémoire de la Commission d'accès à l'information[1] dans le cadre des travaux de la Déclaration de Montréal pour une intelligence artificielle responsable

---

L'intelligence artificielle (IA), de par son recours à des données massives, incluant des renseignements personnels (RPs), et à des processus automatisés de prise de décisions ou algorithmes, soulève plusieurs enjeux en matière de protection des RPs et de la vie privée. Comme l'indique le préambule de la Déclaration de Montréal[2], « *ces machines intelligentes […] cherchent, traitent et diffusent des informations* ». Certains grands principes de protection de RPs universellement reconnus, présentés en annexe, sont parfois remis en question, peut-être même oubliés, lors du développement de nouvelles technologies et plus particulièrement de l'IA.

Il est primordial, comme société, de s'interroger sur les balises que l'on veut instaurer afin, à la fois de permettre le développement d'une technologie prometteuse à plusieurs égards et d'éviter certaines dérives. C'est dans ce contexte que la Commission souhaite participer au débat et formuler certains commentaires au regard des enjeux de protection des RPs et de la vie privée soulevés par l'IA.

Protection de la vie privée et développement de l'IA : deux objectifs conciliables

Même si les lois en matière de protection des RPs devront, à terme, être modifiées afin de répondre plus adéquatement à l'environnement technologique et aux nouveaux enjeux qui en découlent, la Commission considère qu'il n'y a pas d'incompatibilité en soi entre le développement de l'IA et la protection des RPs.

Les principes généraux de protection des RPs universellement reconnus demeurent pertinents et doivent être intégrés à la réflexion lors du processus de développement, mais aussi tout au long de l'utilisation d'un service ou d'un produit qui se « nourrit » notamment de RPs. D'ailleurs, le principe proposé dans le cadre des travaux de la Déclaration de Montréal en matière de vie privée, auquel souscrit la Commission, va dans ce sens :

> « Le développement de l'IA devrait offrir des garanties sur le respect de la vie privée et permettre aux personnes qui l'utilisent d'accéder à leurs données personnelles ainsi qu'aux types d'informations que mobilise un algorithme. »

En fait, le respect des principes de protection des RPs et de transparence des processus peut même contribuer à actualiser d'autres valeurs dans la proposition de la Déclaration

---

1 La Commission d'accès à l'information du Québec (la Commission) a pour mission de promouvoir l'accès aux documents des organismes publics et la protection des renseignements personnels dans les secteurs public et privé, en s'assurant du respect de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, A-2.1; la Loi sur l'accès) ainsi que de la *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ, P-39.1; la Loi sur le privé).

2 https://www.declarationmontreal-iaresponsable.com/la-declaration.

de Montréal. Par exemple, limiter la collecte de renseignements personnels permet d'éviter, dans une certaine mesure, que des décisions soient prises sur la base de renseignements susceptibles d'entraîner une discrimination[3], les renseignements susceptibles d'engendrer ce genre de biais n'étant alors pas connus. De plus, limiter l'utilisation qui peut être faite des renseignements personnels peut participer à nous prémunir contre la propagande et la manipulation afin de favoriser la pensée critique[4].

Propositions

Dans le cadre des présents travaux, la Commission propose quatre éléments susceptibles de contribuer à assurer le respect de la vie privée et de la protection des RPs dans le développement et l'utilisation de l'IA.

1) Responsabiliser les entreprises et les organismes publics

Le principe de responsabilisation en matière de protection de la vie privée implique la reconnaissance du devoir d'une organisation de protéger les RPs qu'elle recueille, utilise ou communique à des tiers. Cela peut se traduire par l'adoption de politiques ou de procédures visant le respect de la loi et suggérant les bonnes pratiques en matière de gestion de la protection de la vie privée. Mais surtout, elle favorise une approche préventive.

Un éventail d'outils existe afin d'aider les développeurs et les utilisateurs d'IA à prendre en compte la vie privée et la protection des RPs dans leurs réflexions et leurs pratiques:

- Évaluation des facteurs relatifs à la vie privée pour déterminer et documenter les risques posés par des projets impliquant l'utilisation de RPs. L'évaluation permet d'identifier de façon préventive les problèmes les plus importants et de trouver des solutions opérationnelles ainsi que des possibilités d'amélioration dès la conception d'un projet. Cela permet la prise en compte des enjeux de vie privée en amont et tout au long du cycle de vie du RP (l'utilisation, la communication, la conservation et la destruction). Par exemple, en IA cela pourrait notamment se traduire par l'utilisation de « jeux de fausses données » pour entrainer l'algorithme d'apprentissage.
- Paramètres de vie privée par défaut : cela implique que les paramétrages les plus stricts sont appliqués par défaut, notamment la minimisation de la collecte la gestion rigoureuse des droits d'accès et des durées de conservation.
- Utilisation de technologies d'amélioration de la confidentialité.
- Désignation d'un responsable interne de la protection des renseignements personnels imputable aux plus hautes instances de l'organisation.
- Transparence, au profit du citoyen, des mesures mises en place.

2) Investir dans le développement de technologies protectrices de la vie privée

[3] Principe lié à la justice dans la proposition de la Déclaration de Montréal : https://www.declarationmontreal-iaresponsable.com/la-declaration.

[4] Principe lié à la connaissance dans la proposition de la Déclaration de Montréal, Ibid.

La Commission estime qu'une part des nombreux investissements dont bénéficie la recherche en IA dans le secteur privé devrait être allouée à la recherche de solutions garantissant la protection de la vie privée.

Dans la mesure où l'IA doit se développer en conformité avec les droits fondamentaux des citoyens et nos valeurs démocratiques, la Commission pense qu'il faut encourager à tous les niveaux et par tous les moyens la recherche et le développement dans ce domaine : créer des chaires de recherche, accueillir et accompagner les entreprises innovantes en la matière, etc.

S'agissant d'un droit fondamental, l'État devrait encourager l'implantation d'entreprises et d'organismes qui développent ou ont recours à l'IA dans le respect du droit à la vie privée. Cela pourrait notamment se concrétiser par des incitatifs économiques (crédits d'impôt, subventions), comme c'est le cas pour d'autres industries.

3) Valoriser les entreprises et les organismes publics qui protègent les renseignements personnels

Les entreprises et les organismes publics qui font l'effort de développer leurs produits et services tout en assurant une protection accrue des RPs devraient être valorisés et mis de l'avant.

Cette valorisation peut se faire par plusieurs moyens. À titre d'illustration, nous pouvons souligner qu'en Europe des programmes de certification sont prévus dans le *Règlement européen sur la protection des données personnelles*. Les certifications ou « labels » seront délivrés par des organismes certificateurs agréés. Les entreprises ou organismes qui méritent cette reconnaissance sur la base de critères objectifs sont ainsi mis de l'avant et profitent d'un avantage concurrentiel très significatif et rassurant pour les personnes (consommateurs, clients, employés, utilisateurs du service, etc.)

4) Moderniser les lois existantes

La Commission considère qu'il est surtout essentiel de moderniser rapidement les lois existantes en matière de protection des RPs. L'autoréglementation ne peut suffire devant les enjeux importants soulevés par l'IA qui pourraient, sans réglementation adéquate, remettre en cause certaines valeurs fondamentales de notre société.

Nos lois existent depuis des décennies et ont besoin d'être repensées afin de mieux s'arrimer aux évolutions du 21e siècle, tout en maintenant leur caractère technologiquement neutre. Il ne s'agit pas d'abandonner ou de renoncer aux principes généraux de protection des RPs universellement reconnus. Cela consiste plutôt à adapter la législation afin de s'assurer que tous les usages et les pratiques, dont certains n'étaient même pas envisageables lors de l'adoption de ces lois, soient couverts et que les citoyens soient mieux protégés et informés. En voici quelques exemples.

- **Préciser la notion de renseignements anonymisés et baliser leur utilisation en certaines circonstances**

Actuellement, plusieurs organisations considèrent respecter les lois en matière de protection des RPs parce qu'elles utilisent des données anonymisées. Tel que le souligne la Commission dans son rapport quinquennal de 2016[5], la question de l'anonymisation des données devient de plus en plus complexe. Certains affirment même qu'il s'agit d'un mythe, surtout dans le contexte de diffusion exponentielle de données de tout ordre et des techniques de plus en plus efficaces de recoupement d'informations. Il y a lieu de se demander s'il ne serait pas pertinent de mieux définir les paramètres permettant de conclure que des renseignements sont anonymisés et si certaines utilisations de ces renseignements ne devraient pas être interdites (ex. : dans le but de dresser des profils discriminatoires ou de cibler des groupes afin de faire de la propagande ou de la manipulation).

- **Préserver le contrôle du citoyen sur ses renseignements personnels et la gestion du consentement**

À titre de fondement des règles relatives à la protection des RPs, il importe de préserver et de réaffirmer ce principe dans les législations à la lumière des nouvelles possibilités offertes par les technologies. Toutefois, à l'heure actuelle le citoyen est souvent laissé à lui-même face à une multitude de choix pouvant être lourds de conséquences au regard de sa vie privée et il ne bénéficie pas toujours d'information claire et suffisante pour lui permettre de faire ces choix. La Commission est d'avis que le fardeau doit être renversé et remis sur les épaules des acteurs qui développent des technologies potentiellement attentatoires à la vie privée.

Actuellement, le consentement du citoyen constitue une des pierres angulaires des régimes de protection des RPs et l'une des façons d'assurer au citoyen le contrôle de ses RPs. Toutefois, celui-ci est de plus en plus critiqué, considérant notamment le caractère incompréhensible et complexe des formules de consentement ou des politiques des entreprises et l'absence de véritable choix qu'ils offrent au citoyen.

C'est pourquoi plusieurs, dont la Commission, croient que cette notion doit être repensée en tenant compte de la réalité numérique et de la multiplication des usages possibles des renseignements personnels.

D'autre part, il importe de prévoir spécifiquement dans ces lois le principe de responsabilisation afin que les entreprises et organismes qui déploient des technologies d'IA intègrent dans leurs pratiques des procédures permettant aux personnes d'exercer leurs droits de façon éclairée et donc de garder le contrôle de leurs RPs. La transparence des pratiques des organisations est également essentielle.

De plus, il importe d'informer et de sensibiliser les citoyens aux enjeux de la protection des RPs afin de les responsabiliser et de favoriser le développement d'un sens critique

[5] COMMISSION D'ACCÈS À L'INFORMATION, *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 sur la *Loi sur la protection des renseignements personnels dans le secteur privé*, septembre 2016.

à l'égard de ces questions. Dans une logique de marché, l'utilisateur de services, étant aussi un citoyen, peut influencer l'offre s'il revendique davantage de produits ou de services respectueux de sa vie privée. Par la revendication de ses droits et par l'expression de choix cohérents avec ceux-ci, il exercera une pression qui, à terme, encouragera l'émergence de pratiques responsables en matière de protection de la vie privée.

- **Décisions automatisées et droit de rectification**

Bien que les législations d'autres juridictions le prévoient, les lois québécoises actuelles n'encadrent pas les décisions automatisées, ce qui soulève plusieurs questions : Comment encadrer la prise de décision automatisée pouvant avoir un impact significatif sur des personnes physiques? Auprès de qui les citoyens peuvent-ils obtenir l'information au sujet des algorithmes (données utilisées, critères et pondération) qui ont mené à la décision les affectant? Devrait-on prévoir la possibilité pour le citoyen d'exiger une intervention humaine dans le cadre d'une contestation ?

En matière de protection des RPs, un amalgame de RPs provenant de diverses sources et interprétés dans un autre contexte que celui de leur utilisation peut engendrer des décisions fondées sur des renseignements inexacts, incomplets ou équivoques. Ces décisions peuvent être lourdes de conséquences et le fardeau de corriger la situation ne devrait pas reposer sur les épaules du citoyen.

De même, l'apparition de nouveaux types de RPs, grâce aux capacités technologiques modernes, suscite de nouveaux enjeux et certaines inquiétudes. Par exemple, celles-ci permettent désormais d'inférer des RPs et de colliger ceux-ci à l'insu des individus (ex. : reconnaissance faciale permettant de décoder les émotions). Peut-on colliger ces renseignements à l'insu de la personne concernée et en tenir compte afin de prendre une décision à son sujet? Comment le citoyen pourrait-il exercer son droit à la rectification de ces renseignements?

Conclusion

Le droit à la vie privée est une valeur fondamentale essentielle à notre société démocratique et à l'autonomie de la personne qu'aucune technologie ne devrait remettre en question. Dans un contexte de développement effréné des technologies et de l'IA, il s'avère indispensable de trouver des solutions visant à concilier le respect de la vie privée et de la protection des RPs, tout en encourageant l'innovation et la recherche.

Les technologies, dont l'intelligence artificielle, doivent se développer au bénéfice de l'humain et dans le respect des droits fondamentaux, dont le droit à la vie privée.

ANNEXE : Quelques enjeux de protection des renseignements personnels

Voici une énumération de quelques principes de protection des RPs et de l'impact des applications d'IA sur ceux-ci :

- **La nécessité** : Ce principe assure que toute collecte et utilisation de RPs se limite à ce qui est nécessaire pour atteindre la finalité recherchée. Dans la mesure où l'IA repose sur la collecte et l'analyse de données massives, incluant des RPs, qu'en est-il du respect du principe de nécessité dans ce contexte? Devrait-on interdire la collecte de certains renseignements dans certains contextes, par exemple pour éviter la discrimination?

- **La finalité** : Ce principe implique que les entreprises et organismes déterminent, avant toute collecte, à quelles fins les RPs seront collectés, utilisés et à qui ils seront communiqués et en informe par la suite les personnes concernées. Or, l'IA nécessite le recours à des données massives de provenances diverses, qui ont parfois été colligées à d'autres fins. Cette utilisation à des fins secondaires de RPs doit-elle être permise et, le cas échéant, de quelle manière devrait-elle être encadrée?

- **Le consentement** : Face à la complexité des nouveaux usages des RPs et des conséquences sur les personnes qui peuvent en découler, est-il encore possible de consentir de façon libre et éclairée? Ce concept est-il toujours adéquat dans le contexte numérique? Sinon, comment renforcer les attributs du consentement et devrait-on recourir à d'autres outils?

- **La confidentialité** : Alors que la confidentialité des RPs doit être la règle, comment mesurer l'efficacité des techniques d'anonymisation et s'assurer qu'il n'y a pas de risques de réidentification, surtout quand il s'agit de RPs sensibles?

- **La conservation et la destruction** : Les RPs doivent être détruits lorsque la finalité ayant mené à leur collecte est atteinte. Comment s'en assurer dans un contexte d'IA?

- **Le droit à l'information et la transparence** : L'IA implique le recours à des algorithmes, soit une suite d'opérations menant à des résultats en ayant recours à différentes données. Lorsque les algorithmes utilisent des RPs, les personnes concernées devraient être informées à la fois des données et des composantes de l'algorithme ayant mené à la prise de décision.

- **Le droit d'accès des personnes concernées** : Suite logique du principe précédent, les personnes doivent pouvoir avoir accès aux RPs qui les concernent et utilisés par un algorithme. Ce droit devrait s'étendre aux données qui, à la suite du recours à l'IA, ont été créées ou inférées à partir de leurs « données brutes » (ex. : liste de préférences).

- **La responsabilité** : Dans un contexte où l'IA peut faire intervenir une multitude d'acteurs au niveau de la collecte, de l'utilisation et de la communication des RPs, qui porte la responsabilité en cas d'atteinte à la vie privée ? Vers qui le citoyen peut-il se tourner pour exercer ses droits ? La responsabilité doit-elle être partagée ? Si oui, sur la base de quels critères?