Commission
d'accès à l'information
du Québec

Québec
Bureau 2.36
525, boulevard René-Lévesque Est
Québec (Québec) G1R 5S9
Téléphone : 418 528-7741
Télécopieur : 418 529-3102

Montréal
Bureau 900
2045, rue Stanley Ouest
Montréal (Québec) H3A 2V4
Téléphone : 514 873-4196
Télécopieur : 514 844-6170

Sans frais : 1 888 528-7741 | cai.communications@cai.gouv.qc.ca | www.cai.gouv.qc.ca

Document de consultation

Intelligence artificielle

Table des matières

EN CE QUI CONCERNE CETTE CONSULTATION

En raison de son rôle d'organisme responsable « d'assurer le respect et la promotion de l'accès aux documents et de la protection des renseignements personnels »[1], la Commission d'accès à l'information du Québec (la Commission) souhaite proposer des principes et des mesures propres à encadrer les enjeux spécifiques relatifs à la protection des renseignements personnels soulevés par le recours à des systèmes d'intelligence artificielle.

Pour que cet énoncé soit en adéquation avec la réalité québécoise et qu'il soit porteur pour l'ensemble des parties prenantes, la Commission souhaite obtenir les commentaires de représentants de l'industrie, des chercheuses et chercheurs du domaine de l'intelligence artificielle et des disciplines connexes, ainsi que des intervenants-clés de la société civile.

C'est à ce titre que la Commission vous transmet le présent document.

Nous vous invitons à commenter les principes proposés dans le présent document en vous posant les questions suivantes :

- **Êtes-vous d'accord avec les principes proposés par la Commission? Sinon, pourquoi?**
- **Est-ce que la mise en application de ces principes soulèverait des enjeux non considérés par la Commission? Le cas échéant, quels ajustements ou pistes de solution devraient être privilégiés?**
- **Selon vous, est-ce que la Commission omet d'inclure des principes ou des éléments importants dans cette proposition? Si oui, quels sont-ils et pour quelle(s) raison(s) considérez-vous qu'ils devraient être inclus?**

Quelques questions plus spécifiques sont ajoutées à même le texte. Nous vous invitons à y réagir également.

Nous vous demandons de bien vouloir communiquer vos commentaires à l'adresse courriel veille@cai.gouv.qc.ca ou par courrier à l'attention de monsieur Martin Carbonneau, agent de recherche au Bureau de la présidence, avant le **20 mars 2020**, à l'adresse suivante :

Commission d'accès à l'information
Bureau 2.36
525, boulevard René-Lévesque Est
Québec (Québec) G1R 5S9

[1] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1, ci-après Loi sur l'accès), article 122.1

Les lignes de texte des sections suivantes ont été numérotées afin de vous permettre d'identifier les passages visés par vos commentaires, pour en faciliter le repérage.

La Commission tient à vous remercier pour la considération que vous porterez à cette consultation.

CONTEXTE

Malgré les nombreux bénéfices que la société québécoise peut anticiper de la part des systèmes d'intelligence artificielle (SIA), force est de constater que leur développement et leur exploitation soulèvent des enjeux importants, notamment en matière de droit à la vie privée et de protection des renseignements personnels.

Générés ou exacerbés par les caractéristiques et les potentialités propres aux SIA, ces enjeux sont parfois intimement liés au respect d'autres droits fondamentaux. La discrimination susceptible de résulter de biais présents dans les algorithmes ou dans le profilage en est un exemple.

L'adoption des lois québécoises de protection de la vie privée précède largement l'émergence des SIA. Certains aspects de ces nouvelles technologies remettent toutefois en question la capacité de ces lois à protéger adéquatement la vie privée des citoyens dans certains contextes.

La Commission est consciente des avantages indéniables promis par l'intelligence artificielle. Sans vouloir proposer des règles propres au recours à ces systèmes, notamment afin de préserver la neutralité technologique de ces lois, elle considère néanmoins que certaines modifications législatives sont requises pour tenir compte de l'incidence de certaines particularités des SIA sur la protection de la vie privée.

Par exemple, plusieurs soulignent que le principe de limitation de la collecte de renseignements personnels à ceux qui sont nécessaires pour une finalité déterminée s'applique difficilement au contexte du développement et de l'utilisation des SIA. Comment alors encadrer et limiter la collecte et l'utilisation de renseignements personnels dans le contexte des SIA? Comment assurer la transparence et l'équité dans le développement et l'exploitation des SIA?

C'est dans ce contexte que la Commission soumet les principes qui suivent.

ENCADRER LA CRÉATION ET L'UTILISATION DE RENSEIGNEMENTS INFÉRÉS

Le cadre législatif actuel couvre uniquement les renseignements qui concernent une personne et qui ont été recueillis par un organisme public ou une entreprise privée. Ces derniers ne peuvent recueillir que les renseignements personnels nécessaires[2].

Certains prétendent que les renseignements inférés[3] par les algorithmes ne sont pas « colligés » par les entreprises et les organismes publics et, par conséquent, y échappent. Or, un renseignement inféré, s'il concerne une personne physique et qu'il permet de l'identifier, est un renseignement personnel. Il devrait donc être soumis à des règles visant à assurer le respect de la vie privée des individus au même titre qu'un renseignement colligé.

Bien que la création et l'inférence de renseignements personnels ne sont pas apparues avec l'intelligence artificielle, celles-ci décuplent les possibilités de croisement entre les différents jeux de données et facilitent les activités de profilage des personnes et l'analyse et la prédiction de leurs comportements.

Ainsi, les renseignements créés ou inférés par les SIA devraient être soumis aux mêmes obligations que les renseignements qui sont colligés par les organisations, notamment le critère de nécessité. Les principes et obligations applicables aux systèmes informatisés en général devraient également s'appliquer de façon explicite aux activités de profilage, d'analyse ou de prédiction. De plus, l'utilisation de certaines catégories de renseignements personnels plus sensibles devrait faire l'objet d'un encadrement plus strict compte tenu des conséquences préjudiciables susceptibles d'en résulter.

La Commission propose les principes suivants :

1. L'inférence ou la création de renseignements personnels à partir d'un algorithme devraient être limitées, en application du critère de nécessité.
2. Les activités de profilage, d'analyse et de prédiction devraient être définies dans la loi. La loi devrait prévoir des conditions et des obligations les encadrant, comme :
    - 2.1. Interdire l'utilisation de certains types de renseignements personnels afin d'effectuer du profilage (ex. : renseignements concernant l'origine raciale ou ethnique, les croyances et les opinions politiques, la santé, l'orientation sexuelle et les renseignements financiers ou biométriques), sauf si certaines conditions prévues dans la loi le permettent;

[2] Voir les articles 64 de la Loi sur l'accès et 5 de la *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, c. P-39.1 (ci-après, la Loi sur le privé).

[3] L'inférence de renseignements est entendue comme la production de nouveaux renseignements à partir de renseignements colligés et détenus préalablement.

2.2. Obliger les entreprises et les organismes à désactiver par défaut les paramètres de profilage, d'analyse et de prédiction pour donner l'occasion aux personnes de consentir ou non à leur activation;

2.3. Obliger les entreprises et les organismes à faire preuve de transparence dans la création ou l'utilisation de renseignements inférés (voir ci-après).

Question : L'article 4 du *Règlement européen de protection des données*[4] (RGPD) présente la définition suivante du profilage : « *[…] toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique* ». **D'après vous, est-ce que cette définition est adéquate? Quels éléments devraient être retenus, retirés ou ajoutés?**

Question : D'après vous, quelles pourraient être les conditions et obligations permettant et/ou encadrant les activités de profilage, d'analyse et de prédiction? Le consentement exprès d'une personne fait-il partie des conditions auxquelles ces renseignements pourraient être recueillis ou utilisés? Est-il une voie réaliste ou souhaitable?

INTERDIRE L'UTILISATION DE RENSEIGNEMENTS PERSONNELS À DES FINS MALVEILLANTES

Malgré l'autonomie apparente des SIA, leur mise en œuvre fait encore l'objet d'une intervention humaine. Les fins poursuivies par les personnes qui développent ou exploitent des SIA peuvent, elles, faire l'objet d'une évaluation.

Dans certains cas, les motivations derrière l'utilisation de renseignements personnels pourraient s'avérer éthiquement inacceptables pour la société, notamment au regard de l'atteinte à la vie privée qu'elles constituent ou de l'atteinte à d'autres droits fondamentaux. D'autres pourraient même se révéler dangereuses pour la vie des personnes.

La Commission propose le principe suivant :

3. Le développement d'un SIA ou l'utilisation de renseignements personnels à l'aide d'un SIA à des fins illégitimes ou avec des intentions malveillantes comme celles de tromper, de discriminer des personnes ou de leur causer du tort devraient être interdits.

[4] Le texte du *Règlement européen de protection des données* est accessible à l'adresse URL suivante : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679

Question : Les concepts de « fins illégitimes » et d'« intentions malveillantes » sont subjectifs. Avez-vous d'autres propositions permettant d'atteindre l'objectif de ce principe ou ces concepts permettraient d'assurer une limitation acceptable de l'utilisation des SIA?

La Commission considère que ce principe pourrait s'appliquer également à tout système informatisé, évitant ainsi de créer une obligation spécifique aux SIA.

UTILISER LES SIA DE MANIÈRE TRANSPARENTE

Les SIA facilitent la prise de décision. Ils permettent l'automatisation complète de certains processus décisionnels. Ils sont également capables d'interactions crédibles avec des personnes physiques sans que ces dernières soient conscientes qu'il s'agit d'un SIA. Ces capacités vont continuer à s'améliorer avec le temps.

Ainsi, l'utilisation de SIA devrait se faire en toute transparence pour que les personnes soient informées qu'elles interagissent avec un SIA et leur permettre d'exercer leurs droits.

La Commission propose les principes suivants :

4. Les entreprises et les organismes publics devraient obligatoirement divulguer l'utilisation d'un SIA, dès lors qu'une personne entre en interaction directe avec celui-ci, au moment d'une collecte de renseignements personnels ou dans le cadre d'une prestation de services;
5. Une personne devrait être informée, au moment d'une collecte de renseignements personnels, que d'autres renseignements seront inférés de manière automatique à son sujet, que les données serviront à des activités de profilage, d'analyse ou de prédiction ou qu'une décision sera prise automatiquement à partir des informations qu'elle fournit;
6. Une personne doit pouvoir exiger obtenir une explication des facteurs et des paramètres les plus importants ayant mené à la prise d'une décision et de la logique du mécanisme de traitement automatisé utilisé pour la prendre, ainsi que de la liste des renseignements personnels utilisés;
7. Le cadre de gouvernance d'une entreprise ou d'une organisation qui utilise un SIA (voir principe 11) devrait être accessible pour qui en fait la demande, ou devrait être diffusé de façon proactive.

ÉTABLIR UN DROIT À LA RÉVISION D'UNE DÉCISION PRISE PAR UN SIA

De nombreuses tâches peuvent être effectuées plus efficacement par les SIA que par les personnes. Toutefois, plusieurs mentionnent le risque qu'un algorithme soit biaisé. La principale raison évoquée est l'utilisation de jeux de données eux-mêmes biaisés lors de l'entrainement des algorithmes. Une décision pourrait aussi être basée sur une prédiction ou une conclusion générée par un algorithme dont le bien-fondé ou la légitimité est discutable ou qui ne prend pas en considération certains éléments pertinents.

Ainsi, lorsqu'un processus implique qu'un SIA prenne une décision produisant des effets juridiques pour un individu ou autrement susceptible d'affecter cette personne de manière significative, celle-ci devrait pouvoir exiger une intervention humaine dans le processus décisionnel. Par ailleurs, les principes d'équité procédurale et les droits de révision ou d'appel déjà prévus continuent de s'appliquer.

La Commission propose les principes suivants :

8. Prévoir le droit d'exiger une révision par une personne physique d'une décision prise initialement par un SIA.

ÉLARGIR LA PORTÉE DU DROIT À LA RECTIFICATION

Le droit à la rectification d'un renseignement personnel implique la démonstration qu'il est inexact, incomplet ou équivoque. Or, il peut être difficile de débattre de ces critères dans le cas de renseignements inférés, surtout par un algorithme de nature prédictive.

Le droit à la rectification tel qu'il est prévu actuellement dans les lois ne couvre pas cette situation. Il devrait être adapté.

La Commission propose les principes suivants :

9. Étendre le droit à la rectification aux situations où la création ou l'inférence de renseignements personnels n'était pas autorisée par la loi (destruction du renseignement);

10. Le droit à la rectification d'un renseignement inféré ne devrait pas inclure une obligation pour la personne concernée de démontrer son caractère inexact, incomplet ou équivoque; **ou**

    Un recours plus spécifique à la nature de ce type de renseignement devrait être prévu, soit le droit de modifier l'inférence, l'opinion, le jugement ou la qualification réalisés par un système automatisé.

ADAPTER LA GOUVERNANCE À LA RÉALITÉ NUMÉRIQUE

Le fait que les SIA soient capables, à divers degrés, de faire preuve d'autonomie n'exonère pas les organisations de leurs responsabilités.

Les entreprises et organismes publics devraient être en mesure de démontrer la prise en charge de leurs responsabilités à l'égard du respect de la vie privée et de la protection des renseignements personnels.

La Commission propose les principes suivants :

11. Obliger les entreprises et les organismes publics à adopter un cadre de gouvernance de la protection des renseignements personnels (accountability). Ce cadre devrait contenir des mesures spécifiques visant à encadrer les enjeux propres à l'utilisation de renseignements personnels dans le contexte d'un SIA.

    Ce cadre de gestion devrait inclure notamment des politiques, des directives et des procédures, des mesures d'évaluation et d'atténuation des risques, des vérifications et audits réguliers, des mesures de sensibilisation et de formation pour les gestionnaires et les employés, des mesures de transparence des pratiques de l'organisation en matière de SIA et la documentation pertinente permettant d'attester du traitement des renseignements personnels par le SIA, de la phase de conception à son déploiement.

    La documentation permettant d'attester des mesures mises en place devrait être mise à jour et conservée. Ces documents devraient être compréhensibles et accessibles;

12. La production d'une *évaluation des facteurs relatifs à la vie privée* (EFVP) devrait être obligatoire préalablement à la mise en œuvre de tout SIA impliquant des renseignements personnels. L'EFVP devrait rendre compte de la circulation des renseignements personnels et des mesures prises pour assurer leur qualité et inclure une évaluation de l'impact algorithmique.

Question : L'EFVP contient généralement : une description de la mise en œuvre d'un système ou d'un processus, une analyse du cycle de vie du renseignement personnel, une vérification de la conformité aux lois de protection de renseignements personnels et une évaluation et une gestion des risques à la vie privée que cette mise en œuvre suscite. D'après vous, est-ce que des tests particuliers (ex. processus de certification) ou des processus d'évaluation supplémentaire (ex. comité d'éthique) devraient faire également partie de l'EFVP, plus généralement, d'un cadre de gouvernance des SIA?

13. Le cadre de gestion, les EFVP et autres audits devraient être révisés périodiquement;

14. Les principes de respect de la vie privée dès la conception (privacy by design) et par défaut (privacy by default) devraient être appliqués lors du développement de tout SIA impliquant des renseignements personnels;

15. La déclaration aux autorités concernées des incidents de sécurité liés à l'utilisation d'un SIA et impliquant des renseignements personnels devrait être obligatoire.

La Commission considère que ces principes pourraient s'appliquer également à tout système d'information.

RENFORCER LES MOYENS DE CONTRÔLE ET D'AUDITABILITÉ

Les organismes de contrôle doivent disposer de pouvoirs d'intervention efficaces lorsqu'une organisation développant ou exploitant un SIA ne se conforme pas à ses obligations légales ou compromet les droits des personnes.

La Commission propose les principes suivants :

16. Les autorités de contrôle, dont la Commission, devraient avoir accès au code des algorithmes à des fins de vérification et de contrôle;

17. Des mesures de sanctions dissuasives devraient pouvoir être imposées par la Commission aux entreprises et organismes en cas de manquement à leurs obligations à l'égard des renseignements personnels, incluant dans le cadre du développement ou de l'exploitation d'un SIA.

PARTICULARITÉS DE LA RECHERCHE ET DU DÉVELOPPEMENT EN INTELLIGENCE ARTIFICIELLE

La recherche appliquée en intelligence artificielle et les phases de développement d'un SIA posent des enjeux particuliers à l'égard de la protection des renseignements personnels.

À titre d'exemple, plusieurs affirment qu'un algorithme sera d'autant plus fiable et exempt de biais que les renseignements qui auront été utilisés dans sa période d'entrainement sont nombreux, diversifiés, exacts et de qualité. Ce besoin de données entre en conflit avec le principe de limitation de la collecte.

Question : Comment traduire le principe de limitation de la collecte dans le contexte de l'utilisation d'un SIA?

Également, il semble qu'il puisse s'avérer difficile, voire parfois impossible, de prévoir quelles seront les finalités de l'utilisation de renseignements personnels dans le cadre de certains développements d'un SIA. Or, cette réalité entre en conflit avec la nécessité de déclarer les fins lors de la collecte de renseignements personnels.

Question : Est-ce que, tout en continuant de favoriser l'obtention du consentement, il serait pertinent et utile de prévoir des circonstances rendant acceptable l'utilisation de renseignements personnels lorsqu'il est impossible de l'obtenir, sous réserve de certaines conditions? Si oui, quelles seraient ces circonstances? Quelles pourraient être ces conditions?

Question : Est-ce que l'utilisation de données anonymisées ou de jeux de données synthétiques pour l'entrainement des SIA devrait être favorisée?

Question : Est-ce que la réidentification de données préalablement dépersonnalisées ou déidentifiées, ou la réidentification délibérée, mais sans nécessité autorisée ou apparente devraient être interdites et sanctionnées?

La Commission s'interroge sur la pertinence que des distinctions soient apportées aux lois en ce qui a trait à la recherche et au développement en intelligence artificielle, aux phases de développement d'un SIA ou à son exploitation par une organisation. L'objectif n'est pas d'inhiber l'avancement de la connaissance et de l'innovation, mais d'encadrer l'utilisation des renseignements personnels afin de réduire l'atteinte à la vie privée des personnes.

Des solutions sont proposées par différents acteurs, notamment :

- Mettre en place un système de bac à sable réglementaire[5];
- Établir un régime de fiducies de données[6].

Question : D'après vous, quelles sont les meilleures solutions pour résoudre les tensions entre la recherche et le développement de SIA? Quelles conditions devraient encadrer ces solutions? Est-ce que d'autres pistes de solution devraient faire partie de la réflexion de la Commission?

Merci pour votre participation à cette consultation.

[5] Le bac à sable réglementaire est un environnement légalement constitué où l'application des règles peut être temporairement suspendue pour certains projets afin de permettre l'innovation technologique, tout en maintenant la supervision d'un organisme de contrôle.

[6] La fiducie de données est un moyen juridique permettant la gestion des données d'un ou de plusieurs bénéficiaires par un fiduciaire, dans l'intérêt des bénéficiaires, selon les règles prévues à l'acte de fiducie. (Inspiré de Element AI & Nesta [2019] *Fiducies de Données : un nouvel outil pour la gouvernance des données*, p.14)