OBSERVATOIRE INTERNATIONAL SUR LES IMPACTS SOCIÉTAUX DE L'IA ET DU NUMÉRIQUE

Laboratoire de CYBERJUSTICE Laboratory

Repenser la protection des renseignements personnels à la lumière des défis soulevés par l'IA

Document de réponse aux questions posées par la Commission d'accès à l'information du Québec dans le cadre de la consultation sur l'intelligence artificielle

Document préparé par Pierre-Luc Déziel, Karim Benyekhlef et Eve Gaumond

Avec la collaboration de Philippe Besse, Philippe Després, Richard Khoury, Mark Likhten et Sylvain Longhais

Avril 2020

OBSERVATOIRE INTERNATIONAL SUR LES IMPACTS SOCIÉTAUX DE L'IA ET DU NUMÉRIQUE

Laboratoire de CYBERJUSTICE Laboratory

Ce document a été préparé dans le cadre de la consultation de la Commission d'accès à l'information du Québec sur l'intelligence artificielle

Document préparé par :

Pierre-Luc Déziel, professeur adjoint à la Faculté de droit de l'Université Laval, coresponsable de l'axe Droit, cyberjustice et cybersécurité de l'Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA).

Karim Benyekhlef, professeur titulaire à la Faculté de droit de l'Université de Montréal, directeur du Laboratoire de cyberjustice et coresponsable de l'axe Droit, cyberjustice et cybersécurité de l'OBVIA.

Eve Gaumond, étudiante à la maîtrise en droit à l'Université Laval, membre chercheure-étudiante de l'OBVIA.

Avec la collaboration de :

Philippe Besse, professeur de mathématiques à l'Université de Toulouse et membre chercheur de l'OBVIA.

Philippe Després, professeur agrégé au Département de physique, de génie physique et d'optique de l'Université Laval et coresponsable de l'axe Santé durable de l'OBVIA.

Richard Khoury, professeur agrégé au Département d'informatique et de génie logiciel de l'Université Laval et membre chercheur de l'OBVIA.

Mark Likhten, avocat, Laboratoire de cyberjustice.

Sylvain Longhais, étudiant à la maîtrise en droit des technologies de l'information à l'Université de Montréal, Laboratoire de cyberjustice.

ISBN 978-2-9818996-0-6

TABLES DES MATIÈRES

INTRODUCTION

Ce document présente les principales observations, réponses et recommandations de l'*Observatoire international sur les impacts sociétaux de l'IA et du numérique* (OBVIA) aux questions posées par la Commission d'accès à l'information du Québec (CAI) à l'occasion de sa consultation sur la protection des renseignements personnels dans un contexte d'intelligence artificielle. L'OBVIA est un espace de discussion et de réflexion qui rassemble plus de 200 chercheuses et chercheurs dont l'objectif principal est de maximiser les effets positifs de l'IA. La problématique du droit à la protection de la vie privée est au coeur des efforts de l'OBVIA, notamment par le biais de son axe "Droit, cyberjustice et cybersécurité".

Suite à la réception du document de consultation de la Commission, l'OBVIA a entamé un processus de consultation auprès de certains de ses membres dans le but de recueillir les réactions d'experts provenant de divers horizons disciplinaires. Ainsi, le présent document regroupe les avis de chercheurs et chercheuses en droit, en génie informatique et en santé. Le Laboratoire de cyberjustice de l'Université de Montréal, un partenaire de l'Observatoire, a également soumis des commentaires étoffés qui ont été intégrés au présent document.

Les principaux objectifs du document sont :

- (1) D'offrir une synthèse, qui soit intelligible pour le plus grand nombre, des enjeux juridiques et technologiques associés à la protection des renseignements personnels (RP) à l'ère de l'intelligence artificielle.
- (2) Et de proposer une approche concertée et interdisciplinaire pour une meilleure protection des renseignements personnels à l'ère de l'intelligence artificielle au Québec.

Il va sans dire que l'effort actuel de réforme des lois visant la protection des renseignements personnels au Québec dans le but de faire face aux défis occasionnés par l'intelligence artificielle sur le plan de la vie privée soulève des problèmes complexes et particuliers. Toutefois, une telle réforme ne peut, selon nous, se satisfaire d'une approche étroite, qui ne se contenterait que de répondre aux enjeux qu'engendre aujourd'hui le développement de l'intelligence artificielle. Elle doit, au contraire, faire preuve de prévoyance et imaginer des lois qui résisteront au test du temps et pourront s'adapter aux défis qui seront soulevés par l'IA – ou par d'autres technologies – dans l'avenir.

Pour ce faire, il nous semble important de concentrer les efforts de réforme sur l'aspect matériel de la loi, c'est-à-dire la protection des renseignements personnels. À cet effet, nous croyons qu'il faut réaffirmer l'importance des principes fondamentaux des lois québécoises sur la protection des renseignements personnels, tout en leur apportant quelques ajustements afin qu'ils demeurent adaptés aux nouveaux défis technologiques qui se présentent. Nous pensons aussi que la réforme visée doit

expressément reconnaître la protection du droit à la vie privée comme un droit fondamental permettant l'affirmation d'autres droits fondamentaux.

Une telle démarche nous semble plus adéquate que l'adoption d'une approche IA-centriste qui s'intéresserait surtout aux notions de profilage, de personnalisation ou de prédiction. Une approche, qui demeurerait neutre au plan technologique, permet de mieux résister au test du temps et d'éviter certains écueils définitionnels qui peuvent nuire à la mise en oeuvre de la loi. Par conséquent, nous considérons que la position de la Commission, qui semble écarter la possibilité d'inclure une définition de l'intelligence artificielle dans le cadre de la Loi sur la protection des renseignements personnels dans le secteur privé, L.Q, chapitre P-39.1 (LPRPSP), est judicieuse.

Pour faciliter la lecture de notre document de réponse, ce dernier reprendra d'abord les questions d'ordre général explicitement posées dans le document de consultation. Nous développons ensuite certaines thématiques plus précises qui regroupent certains des principes proposés par la Commission. La seconde partie portera donc sur le principe de limitation et la question des fins légitimes. La troisième partie s'intéressera, elle, à la thématique du contrôle individuel sur les renseignements personnels et abordera certains des principes - consentement, accès à l'information, exactitude - qui permettent d'asseoir ce contrôle. La quatrième partie est consacrée à l'enjeu de la responsabilité et de l'imputabilité des entités qui traitent des renseignements personnels. La cinquième et dernière partie offre des réponses à certaines des questions plus spécifiques posées par la Commission dans son document de consultation. Tout au long du document, des recommandations précises sont formulées. Celles-ci sont par ailleurs regroupées sous la forme d'une synthèse à la fin du document.

1. LES QUESTIONS D'ORDRE GÉNÉRAL

Dans son document de consultation, la Commission formule trois grandes questions d'ordre général. L'objectif de cette section est d'apporter certains éléments de réponses à ces questions, qui feront l'objet de développements plus conséquent dans la suite du document.

- **Êtes-vous d'accord avec les principes proposés par la Commission ? Sinon, pourquoi ?**
  - De manière générale, les principes proposés par la Commission constituent une avancée en matière de réglementation des systèmes d'intelligence artificielle (SIA). Cependant, ils soulèvent aussi, à certains moments, des enjeux de réalisme dans leurs applications.
  - Par exemple, le principe 6 - qui porte sur le droit à l'explication - est difficile à mettre en pratique. En effet, l'interprétabilité des SIA en est encore à ses balbutiements. Bien qu'il soit possible de nommer des techniques de traitement

de l'information (par ex. apprentissage profond), il demeure souvent difficile d'expliquer la décision d'une façon claire et limpide.

- De même, le principe 16 - qui porte sur l'accès aux codes des algorithmes - semble plus ou moins bien adapté aux algorithmes par apprentissage. Ceux-ci demeurent, somme toute, plus ou moins insignifiants sans les données sur lesquels ils ont été entraînés. Par conséquent, les données devraient aussi, peut-être même *surtout*, être disponibles à des fins de transparence.
- De plus, on peut faire quelques remarques quant au réalisme dans l'application de certains principes. Il y a lieu de considérer, par exemple, que maintenir le consentement exprès comme seule option de licéité du traitement n'est pas viable lorsque l'on parle d'utilisation de SIA. Il est ainsi possible d'envisager un élargissement des critères de licéité du traitement de l'information, notamment lorsque celui-ci porte sur des renseignements dépersonnalisés.

- **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 ?**

- La mise en application de certains principes soulève des enjeux qui ne sont pas considérés par la Commission. C'est notamment le cas de la nécessité de définir juridiquement des termes qui ont une grande importance et qui sont bien souvent abordés comme une évidence alors qu'ils méritent une attention particulière. C'est notamment le cas du droit d'accès, qui subordonne le droit de révision et le droit de rectification des renseignements personnels, et peut avoir des impacts sur la transparence des opérateurs utilisant des SIA. À des fins de pertinence du cadre réglementaire, définir le droit d'accès et en fixer les contours est primordial. De la même façon, le terme de traitement de données doit être défini juridiquement pour appréhender les problématiques posées par l'utilisation de SIA. Il est à la base d'une réglementation comme celle-ci.
- Enfin, les principes proposés doivent former un ensemble cohérent. On peut avoir parfois trop l'impression d'avoir affaire à une série de principes qui ne sont pas reliés entre eux, mais qui visent plutôt à combler certaines déficiences du cadre réglementaire existant.

- **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) raisons considérez-vous qu'ils devraient être inclus ?**

- Il aurait été préférable d'aborder la question du stockage de la donnée. En effet, comme soulevé dans le Livre blanc de la Commission européenne sur l'intelligence artificielle, il faut se préparer à l'arrivée de nouveaux systèmes de

stockage de données dans un futur proche.[1] Cela va très certainement induire de nouvelles problématiques juridiques qu'il convient d'anticiper. C'est notamment le cas du *Edge Computing*[2] consistant en un traitement décentralisé de la donnée.

- De plus, on ne trouve pas de références explicites aux bonnes pratiques ou usages issus de l'industrie. Il est dommage de ne pas saisir l'occasion d'impliquer des acteurs privés dans cette réglementation. En effet, de plus en plus de normes sur le sujet des SIA émergent, que ce soit par le biais de standards ISO ou bien des principes FAIR qui visent à permettre un meilleur accès et une meilleure visibilité des données.
- De la même façon, on omet d'aborder un principe possible de certification basé sur une réglementation *by design* et des procédures d'audit continu afin de s'assurer que la réglementation soit bien respectée. D'ailleurs, il est même possible d'imaginer que l'utilisation d'un SIA soit subordonnée à la nécessité d'y avoir recours afin de réduire les risques liés à leur utilisation.

2. LE PROFILAGE ET LE PRINCIPE DE LIMITATION : LA QUESTION DES FINS LÉGITIMES ET ACCEPTABLES

Cette section s'intéresse aux principes 1, 2 et 3 du document de consultation de la Commission. Le principe 1 porte sur l'application du critère de nécessité aux processus d'inférence ou de création de renseignements personnels par le biais de systèmes d'intelligence artificielle. Le principe 2 propose l'ajout d'une définition précise des activités de profilage, d'analyse et de prédiction qui peuvent conduire à la création ou à l'inférence de renseignements personnels. Le principe 3 avance l'idée selon laquelle la loi devrait interdire le développement d'un système d'intelligence artificielle à des fins illégitimes ou avec des intentions malveillantes.

Ces principes interpellent des enjeux définitionnels, notamment en ce qui a trait aux notions de renseignements personnels et de profilage, qui doivent d'abord faire l'objet d'un traitement attentif (2.1). Ensuite, l'application du critère de nécessité soulève la question de la pertinence du principe de limitation de la collecte, de l'utilisation et de la divulgation de renseignements personnels dans un contexte d'intelligence artificielle. L'analyse de ce principe nous amène naturellement à la problématique des fins légitimes et acceptables en droit canadien (2.2.). Finalement, la question de l'acceptabilité et de la légitimité du profilage doit être réfléchie en fonction des effets du profilage et non de la nature des renseignements à partir desquels il opère.

---

[1] Commission Européenne, *Livre blanc de la Commission européenne, intelligence artificielle, une approche européenne axée sur l'excellence et la confiance, COM(2020) 65 final*, Bruxelles, 19 février 2020 à la p 2, en ligne : https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf.

[2] Le *Edge Computing* est un modèle dans lequel les ressources informatiques et de stockage sont décentralisées en « Cloudlets », ou micro-data centers (par opposition à la centralisation du Cloud Computing) qui se trouvent aux « bords » d'internet, c'est-à-dire à proximité de la source des données, donc des objets connectés. Voir ; MAHADEV SATYANARAYANAN , «The Emergence of Edge Computing» '(2017) 50 *Computer* 1 aux pp 30-39, en ligne : http://www.cs.cmu.edu/afs/cs.cmu.edu/user/satya/Web/docdir/satya-edge2016.pdf

2.1 Les enjeux définitionnels: inférence, profilage et renseignements personnels

L'examen des principes 1 à 3 du document de consultation de la Commission exige une analyse plus fine des notions d'inférence et de profilage, qui nous renvoient elles-mêmes à la définition de ce qu'est un renseignement personnel en droit québécois. Dans cette sous-section, nous nous affairons donc à clarifier ces termes. À cet effet, nous verrons d'abord que la *LPRPSP* devrait explicitement reconnaître une inférence ou une prédiction comme un renseignement personnel, et que la définition même du renseignement personnel doit être modifiée de manière à assurer la protection des renseignements qui sont dépersonnalisés. Ensuite, nous verrons que la définition de la notion de profilage avancée par le *Règlement général sur la protection des données (RGPD)* est adéquate, mais qu'elle doit aussi être replacée dans le contexte particulier du *RGPD* pour prendre tout son sens. Ainsi, nous pensons qu'avant d'envisager de transposer cette définition en droit québécois, certains ajustements plus systémiques doivent être apportés.

Les limites de la définition actuelle de renseignement personnel

Il serait une erreur de ne considérer les pratiques de profilage, de création ou de prédiction qu'à partir de la notion de renseignement personnel telle qu'elle est présentement définie en droit québécois ou canadien. En effet, cette définition est, à notre avis, trop étroite pour bien rendre compte de certains des enjeux que soulève l'utilisation de SIA à des fins de profilage. Les limites de la définition actuelle se situent à deux niveaux. D'abord, elle n'inclut pas clairement les renseignements personnels qui ont été dépersonnalisés. Ces renseignements peuvent être utilisés dans la création de profils génériques qui peut avoir une incidence sur la vie des personnes.[3] Ensuite, la *LPRPSP* n'indique pas clairement qu'une inférence, une prédiction ou une évaluation est un renseignement personnel. Dans la mesure où une inférence, une prédiction ou une évaluation comporte des informations qui portent sur une personne identifiable, il serait *a priori* naturel de les qualifier de renseignements personnels. Toutefois, on pourrait aussi affirmer que la nature plus hypothétique que factuelle d'une prédiction, d'une inférence ou d'une évaluation fragilise l'idée qu'il s'agisse bel et bien d'un "renseignement".[4] Afin d'éviter une telle interprétation, nous considérons que la loi québécoise devrait clairement préciser que les prédictions, inférences ou évaluations faites à partir des renseignements personnels d'une personne doivent aussi être considérées comme des renseignements personnels.

---

[3] Pierre-Luc Déziel, « Les limites du droit à la vie privée à l'ère de l'intelligence artificielle : groupes algorithmiques, contrôle individuel et cycle de traitement de l'information », (2018) 30 : 3 *Cahiers de Propriété Intellectuelle* 827

[4] Sur ce point, il convient peut-être de préciser que la définition de renseignement personnel que l'on trouve dans la *Loi sur les renseignement personnel*, LRC 1985, c P-21 inclut les "les idées ou opinions d'autrui" sur une personne identifiable.

Afin de bien saisir la portée de ces deux limites, il convient de brièvement revenir sur la définition de la notion de renseignement personnel et à la protection qui lui est offerte en droit québécois. La *LPRPSP* protège les renseignements qui peuvent être qualifiés de renseignements personnels. À son article 2, la *LPRPSP* définit un renseignement personnel comme "tout renseignement qui concerne une personne physique et permet de l'identifier." Notons que cette définition couvre aussi les renseignements qui, combinés avec d'autres renseignements, permettent d'identifier une personne physique. À première vue, les renseignements qui ne sont pas qualifiés de "personnels", notamment parce qu'ils ne permettraient pas d'identifier une personne, tombent à l'extérieur de la sphère de protection de la loi. À cet effet, les renseignements qui sont *dépersonnalisés*, c'est-à-dire transformés de manière à ne plus raisonnablement permettre l'identification des personnes, ne seraient pas considérés comme des renseignements personnels au sens de la loi et leur collecte, utilisation ou divulgation ne seraient pas soumises aux exigences de la loi.[5]

Plusieurs études démontrent toutefois que le traitement de données qui ne sont pas *a priori* identificatoires peut néanmoins mener à l'identification des personnes[6] et que les renseignements dépersonnalisés peuvent facilement être utilisés de manière à réidentifier les personnes sources[7]. Il peut ainsi être difficile pour les entreprises de déterminer, à l'avance, si un renseignement non identificatoire ou dépersonnalisé doit être qualifié de renseignement personnel au sens de la loi. Sur ce point, notons aussi que la jurisprudence canadienne et les différentes lois de protection des renseignements personnels sur la santé des provinces adoptent différents standards qualitatifs permettant d'apprécier le risque de réidentification. Il peut s'agir la "forte possibilité"[8] de la réidentification des personnes, de la "facilité" ou de la "raisonnabilité" de la capacité de réidentification.[9]

Cette difficulté, qui crée une incertitude nuisant à l'effectivité de la protection offerte par la loi, doit être dissipée. À notre avis, la définition du renseignement personnel doit

---

[5] Cette limite est aussi considérée par le Commissariat à la protection de la vie privée du Canada (CPVP) au point 8 de son document de consultation sur l'intelligence artificielle. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Consultation sur les propositions du Commissariat visant à assurer une réglementation adéquate de l'intelligence artificielle*, Janvier 2020, Ottawa, en ligne : https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultation-ai/pos_ai_202001/. [CPVP] Notons aussi qu'au considérant 26, le *Règlement général sur la protection des données* exclut les données anonymisées de sa sphère de protection. CE, *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)* [2016] JO, L 119/1. [RGPD]

[6] PAUL OHM, « Broken Promise of privacy : responding to the surprising failure of anonymization » (2010) 57 *UCLA Law Rev* 1701 aux pp 1717-1723. JONATHAN MAYER, PATRICK MUTCHLER ET JOHN C. MITCHELL, « Evaluating the privacy properties of telephone metadata » (2016) 113:20 *Proceedings of the National Academy of Sciences* 5536.

[7] LUC ROCHER, JULIEN M HENDRICKX ET YVES-ALEXANDRE DE MONTJOYE, « Estimating the success of re-identifications in incomplete datasets using generative models» (2019) 10 *Nature Communications* 3069. YVES-ALEXANDRE DE MONTJOYE, et al., « Unique in the shopping mall: On the reidentifiability of credit card metadata » (2015) 357: 6221 *Science* 536.

[8] *Gordon c. Canada (Santé)*, 2008 CF 258

[9] KARIM BENYEKHLEF ET PIERRE-LUC DÉZIEL, *Le droit à la vie privée en droit québécois et canadien*, Montréal, Yvon Blais, 2018 à la p. 341. PIERRE-LUC DÉZIEL, *La protection des renseignements personnels sur la santé au temps de la biosécurité*, Montréal, LexisNexis, 2018 à la p. 189 et s.

être claire et facilement interprétable par les entreprises. Dans sa forme actuelle, le critère selon lequel un renseignement doit *permettre l'identification* d'une personne physique est une entrave à cette interprétation. Ainsi, nous croyons que la *LRPSP* devrait clairement indiquer qu'un renseignement personnel "dépersonnalisé" demeure un renseignement personnel et encadrer le traitement de ces renseignements. Notons, sur ce point, que la Commission semble déjà considérer qu'un renseignement dépersonnalisé, codé ou anonymisé conserve son caractère personnel.[10] Nous considérons néanmoins que cette interprétation devrait être clairement précisée dans la loi.

Cette précision engendre toutefois deux questions plus larges. Dans un premier temps, s'il est établi qu'un renseignement dépersonnalisé demeure un renseignement personnel et qu'il doit faire l'objet d'un encadrement légal, il est nécessaire de se demander si cet encadrement doit être plus souple et flexible que celui réservé aux renseignements personnels en général. En d'autres mots, il convient de déterminer si les obligations s'imposant au traitement de renseignements dépersonnalisés doivent être plus permissives que celles visant le traitement de renseignements personnels identificatoires.[11] À notre avis, cet assouplissement est souhaitable et pourrait, par exemple, prendre la forme d'une autorisation de traitement qui s'appuierait sur d'autres critères de licéité que le consentement.[12] Toutefois, toutes tentatives de réidentification délibérée et sans nécessité apparente devraient être proscrite[13].

Dans un second temps, le fait d'établir deux régimes distincts de traitement pose, ici aussi, la question de la capacité de situer la ligne de démarcation entre un renseignement personnel dit "identificatoire" et un renseignement personnel dit "dépersonnalisé". En d'autres mots, à partir de quel moment un renseignement personnel peut être qualifié de dépersonnalisé? Il semble difficile d'établir de manière précise et absolue où se situe cette limite. Néanmoins, nous considérons que la pluralité de critères qui parsèment la jurisprudence canadienne et québécoise[14] ne fait qu'obscurcir davantage cette ligne de partage. Ainsi, nous croyons que la loi devrait identifier un critère unique permettant d'établir à quel moment un renseignement personnel peut être qualifié de dépersonnalisé. Évidemment, dans la mesure où les critères actuels sont de nature qualitative, une certaine incertitude subsistera. Toutefois, le fait d'adopter un critère unique devrait sans doute apporter une certaine forme de précision.

---

[10] COMMISSION D'ACCÈS À L'INFORMATION, site Web de la Commission, dans l'espace "chercheur" en ligne : https://www.cai.gouv.qc.ca/chercheurs/informations-complementaires/

[11] Cette question est abordé par le Commissariat à la protection de la vie privée du Canada (CPVP) au point 8 de son document de consultation sur l'intelligence artificielle. CPVP, *supra* note 5.

[12] Voir *infra*, point 3.1

[13] Voir, *infra* point 5, en réponse à la question posée la Commission à la page 8, ligne 244, de son document de consultation.

[14] *Supra* notes 8 et 9.

Sur ce point, il peut être intéressant de noter que les textes ou projets de loi américains et européens semblent opter pour un critère de "raisonnabilité". En effet, le *Data Care Act* et le *Algorithmic Accountability Act* de l'administration fédérale américaine considèrent que les renseignements "linked, or reasonably linkable" à un consommateur ou à ses outils informatiques sont des renseignements personnels[15]. De plus, le *California Consumer Privacy Act* prévoit quant à lui qu'une donnée qui "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" constitue une information personnelle[16]. De plus, le considérant 26 du *RGPD* propose une approche contextuelle articulée en fonction d'un critère de raisonnabilité :

> Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci.[17]

Par ailleurs, dans le but de faciliter l'arrimage entre le droit à la protection des renseignements personnels et les réalités de l'intelligence artificielle, nous croyons aussi que les inférences, profils, prédictions et résultats de décisions automatisées devraient être considérés comme des renseignements personnels au sens des lois de protection des renseignements personnels s'ils concernent une personne physique. Notons que le *California Consumer Privacy Act* prévoit déjà que certaines inférences doivent être considérées comme étant des renseignements personnels :

> "Personal information" means et […] (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes[18].

Cette position semble aussi s'arrimer à la jurisprudence canadienne qui considère qu'une évaluation générée par un outil actuariel doit être considérée comme un renseignement concernant une personne.[19] À notre avis, l'abandon du critère selon

---

[15] ÉU, Bill S 2961, *Data Care Act of 2019*, 116e Cong., 2019 à l'art 2(3) [*Data Care Act*] ; ÉU, Bill HR 2231 *Algorithmic Accountability Act of 2019*, 116e Cong., 2019 à l'art 10. [*Algorithmic Accountability Act*].

[16] ÉU, AB-375, *California Consumer Privacy Act of 2018*, 2017-18, Reg Sess. Cal, 2018, art 1798.140. (o) i) [CCPA]

[17] RGPD, *supra*, note 5, considérant 26.

[18] CCPA, *supra*, note 16, art. 1798.140. (o) (1) (K)

[19] Voir sur ce point *Ewert c. Canada*, [2018] 2 RCS 165. Il est sans doute important de préciser que cette conclusion repose sur l'interprétation de l'expression "exactitude des renseignements concernant les délinquants" que l'on trouve dans la *Loi sur le système correctionnel et la mise en liberté sous condition*, LC 1992, c 20.

lequel un renseignement devait permettre d'identifier une personne physique pour être considéré comme un renseignement personnel doit faire en sorte que les renseignements rendus non identifiables (dépersonnalisés, anonymisés et pseudonymisés) s'inscrivent désormais dans le champ d'application des lois sur la protection des renseignements personnels. Une telle approche a aussi été retenue par le Japon[20] et semble favorisée par la Commissariat à la protection de la vie privée du Canada dans le cadre de la réforme de la *Loi sur la protection des renseignements personnels et les documents électroniques*.[21]

Les activités de profilage, d'analyse et de prédiction

Au principe 2 de son document de consultation, la CAI indique que les activités de profilage, d'analyse et de prédiction devraient être définies et encadrées. Nous sommes en accord avec cette volonté. Cependant, dans une perspective de neutralité technologique, nous croyons que les définitions entourant ces activités devraient être plus larges et englobantes. L'*Algorithmic Accountability Act* et le RGPD identifient certains types de traitements de renseignements personnels qui comportent un niveau de risque plus important et qui requièrent d'être encadrées par des dispositions particulières.

Le droit Québécois pourrait adopter une approche similaire. Inspirés par l'*Algorithmic Accountability Act*[22] et le RGPD[23], nous croyons que les traitements suivants devraient être considérés comme des traitements de renseignements personnels à haut risque auxquels s'appliquent certaines dispositions particulières.

a) Traitement de renseignements personnels, automatisés ou non :

   i) qui pose un risque important à la vie privée ou à la sécurité des renseignements personnels d'une personne compte tenu de la nouveauté de la technologie employée ou du contexte, de la finalité et de la portée de son utilisation;

   ii) qui implique des données sensibles à l'égard d'un nombre important d'individus.

      1) Les données à caractère personnel qui révèlent 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, des données concernant la vie

---

[20] JAPON, *Amended Act on the Protection of Personal Information (tentative translation)*, 2016, art 2 (9), en ligne : https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf

[21] CPVP, *supra* note 5

[22] *Algorithmic Accountability Act*, *supra* note 15, art 7,8.

[23] RGPD, *supra* note 5, art 35 (3)b. art. 35.

> sexuelle ou l'orientation sexuelle d'une personne physique ainsi que les données à caractère personnel relatives à des condamnations pénales et à certaines infractions sont considérées comme des données sensibles ; [24]

b) Traitement de renseignements automatisés :

> i) qui évalue de manière systématique et approfondie des aspects personnels concernant des personnes physiques et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;
>
> ii) qui risque de manière importante d'entraîner ou de contribuer à des décisions inexactes, injustes, partiales ou discriminatoires compte tenu de la nouveauté de la technologie employée, du contexte, de la finalité et de la portée de son utilisation,

c) Surveillance systématique à grande échelle d'une zone accessible au public.

Le traitement de renseignements personnels à haut risque devrait être une notion charnière, autour de laquelle s'articulent d'autres droits et principes auxquels la notion peut être rattachée.

Par exemple, en Europe, la notion de profilage occupe une place centrale dans l'architecture du *RGPD,* puisqu'elle est directement interpellée par l'article 21, qui porte sur le droit d'opposition, et l'article 22 qui s'intéresse à la prise de décision automatisée, y compris le profilage. Par ailleurs, il importe de souligner que l'article 21 renvoie lui-même à l'article 6 qui définit les critères de licéité du traitement et présente le consentement comme *une* des conditions qui peuvent fonder le caractère licite du traitement de l'information. Nous reviendrons plus loin[25] sur ces différentes notions sur lesquelles se penche la Commission dans son document de consultation et qui devraient, à notre avis, être développées de manière à former un ensemble cohérent.

Toutefois, auparavant, il importe d'apporter quelques précisions au sujet de la définition de profilage prévue à l'article 4 du *RGPD* sur laquelle la Commission sollicite l'opinion des répondants :

> «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,

[24] RGPD, *supra* note 25, art 35 (3)b.

[25] Voir la partie 3.

> les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique;

D'emblée, il convient de préciser que cette définition poursuit à notre avis un double objectif. Le premier est intrinsèque, puisqu'il s'agit de donner une définition en droit du traitement de renseignements personnels permettant de prédire et d'analyser le comportement, les réactions ou encore les préférences d'une personne.[26] La recrudescence de ce type de pratiques est favorisée par le développement des SIA car ceux-ci permettent d'analyser un grand nombre de données afin d'établir et d'affiner un profil individualisé relatif à une personne. Il est donc effectivement primordial que le droit puisse appréhender de telles pratiques et cela passe par une définition suffisamment large qui encadre les différentes techniques de traitement de données utilisées, mais également les éléments personnels que l'activité de profilage cherche à mettre en lumière. Il faut donc constater qu'intrinsèquement, la définition du profilage telle que fournie par l'article 4 du *RGPD* est satisfaisante puisqu'elle ne vise pas un traitement en particulier et ne limite pas les profils personnels résultant de ce profilage.

Toutefois, deux précisions méritent d'être apportées. D'abord, il convient de garder en tête que la problématique du profilage ne doit pas uniquement être abordée en fonction des données à partir duquel il opère ou du type d'inférences qu'il entend générer, mais bien des effets qu'il entend produire. Une interdiction de recourir à des renseignements sensibles dans le cadre d'activités de profilage ou de catégorisation pourrait avoir un effet contraire à celui escompté. En effet, certaines techniques de mitigation des biais nécessitent l'utilisation de ce renseignement sensible pour amoindrir les effets discriminatoires et assurer un traitement plus équitable lors d'une activité de profilage. Par ailleurs, le fait de discriminer en fonction de certaines caractéristiques sensibles comme le sexe ou l'origine ethnique n'est pas qu'une mauvaise chose, cela peut également être souhaitable. Par exemple, dans un contexte de médecine personnalisée où l'on veut profiler pour donner le bon traitement à la bonne personne, l'origine ethnique du patient peut par être utilisée pour prendre des décisions plus éclairées. Ensuite, une approche qui s'attaque aux résultats discriminatoires nous semble plus intéressante qu'une approche fondée sur le type de renseignement en raison de la notion de proxy. Cette notion fait en sorte que certaines discriminations surviennent même lorsque toutes les informations qui semblent révéler l'appartenance d'une personne à un groupe à l'égard de qui la discrimination est interdite ont été éliminées des bases de données.

La deuxième précision porte sur le fait que l'article 4 limite le profilage à « toute forme de traitement automatisé […] » Ainsi, la définition est surtout taillée pour s'adapter à l'utilisation de SIA. Par conséquent, tous les traitements que l'on pourrait qualifier de manuels se voient alors exclus de la définition visée par l'article 4. Même s'il tend à devenir de plus en plus rare, le profilage peut être fait de manière entièrement

[26] Voir à ce titre le billet portant sur le sujet par la CNIL : https://www.cnil.fr/fr/profilage-et-decision-entierement-automatisee.

manuelle à petite échelle[27]. Si le profilage fait à partir de SIA implique un traitement automatisé, quelle est la place des étapes impliquant un traitement manuel puisque les deux peuvent être combinées ? Il ne s'agit donc pas d'oublier une partie des enjeux en considérant que la technologie a fait ou fera disparaître les pratiques manuelles de profilage. Dès lors, ne faut-il pas incorporer ces traitements manuels dans la définition en retirant la caractéristique d'automatisation du traitement ?

Le deuxième objectif de cette définition de profilage est de compléter d'autres définitions de l'article 4 afin de faire du *RGPD* un cadre réglementaire qui soit homogène. Ainsi, elle est intimement liée à la définition de « traitement» qui se trouve aussi à l'article 4:

> Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel, tels que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Les techniques de profilage reprennent des opérations de traitements qui sont envisagées par l'article 4. En effet, profiler c'est structurer des jeux de données, rapprocher, interconnecter des renseignements personnels; autant de termes qui sont prévus par la définition du traitement de données dans le *RGPD*. On pourrait d'ailleurs multiplier les exemples, et ce notamment avec la définition même de la donnée personnelle qui est prévue dans le *RGPD* et à laquelle la définition de profilage se rattache.

Par conséquent, si la définition de profilage proposée par le *RGPD* peut sembler adéquate à l'utilisation de SIA malgré les réserves émises quant à la problématique du traitement manuel des données et des *effets* discriminatoires du profilage, il faut d'abord s'assurer qu'elle s'adapte au droit québécois encadrant les renseignements personnels notamment en ce qui a trait au traitement de la donnée.

---

[27] On fait ici référence aux travailleurs du clic. On peut les définir comme des travailleurs payés à la tâche et dont le travail consiste à annoter, étiqueter, corriger ou encore trier des données dans le but d'entraîner ou de tester des SIA. Pour en savoir plus, voir les travaux d'Antonio Casilli et notamment : Paloa Tubaro, Antonio A. Casilli, « Micro-work, artificial intelligence and the automotive industry », (2019) 46 *Journal of Industrial and Business Economics* aux pp 333-345, en ligne :https://link.springer.com/epdf/10.1007/s40812-019-00121-1?author_access_token=zS9GZQdmKoQncYduy7kuWPe4RwlQNchNByi7wbcMAY7vbypDmaHTsETWibRyHNOxNsDkGt3B_OV9Sn5HtsWcKLlq3_FBd2_qQvkOmScsYUvFR3QFlGnAestialvevVFz74K7f96FCpSaE23r9ydcSg%3D%3D, Antonio A. Casilli, « Digital Labor : travail, technologies et conflictualités. Qu'est-ce que le digital labor ? » (2015) Editions de l'INA aux pp 10-42, en ligne : https://halshs.archives-ouvertes.fr/halshs-01145718/document

RECOMMANDATIONS RELATIVES AU PRINCIPE # 1 DU DOCUMENT DE LA CAI

1. Le critère en vertu duquel une donnée doit permettre l'identification pour être considéré comme un renseignement personnel devrait être abandonné ;

2. Les inférences, profils, prédictions et résultat de décisions automatisées devraient être considérés comme des renseignements personnels s'ils concernent une personne physique ;

3. Les renseignements rendus non identifiables devraient être couverts par les lois de protection des renseignements personnels, même si une certaine souplesse en vue de leur utilisation peut être accordée.

4. L'inférence de renseignements personnels à partir d'un algorithme ainsi que les activités de profilage, d'analyse et de prédiction devraient être encadrés par le biais de la notion de traitement de renseignement personnel à haut risque.

2.2 LE PRINCIPE DE LIMITATION DE LA COLLECTE: NÉCESSITÉ ET LICÉITÉ DU TRAITEMENT

Le principe 1 proposé par la Commission dans son document de présentation porte sur la pertinence d'appliquer le critère de nécessité aux renseignements inférés ou crées à partir d'un algorithme. En droits québécois et canadien, le critère de nécessité est une des deux composantes du principe de limitation de la collecte, de l'utilisation et de la communication de renseignements personnels. Le second critère est celui de la licéité du traitement de l'information, qui renvoie directement à la thématique de l'acceptabilité et de la légitimité des fins visées par le traitement de l'information. La Commission aborde cette thématique de la légitimité du traitement de l'information au point 3 de son document de consultation. Ainsi, nous nous proposons, dans cette sous-section, de brièvement revenir sur le principe de limitation tel que défini en droits québécois et canadien, et ce, dans le but de mieux saisir la portée des principes 1 et 3 proposés par la Commission.

Les lois québécoises de protection des renseignements personnels requièrent que les entreprises et les organisations qui traitent des renseignements personnels à des fins commerciales adoptent une approche minimaliste à l'égard des renseignements personnels. Cette approche minimaliste se traduit par l'application du principe de limitation sur les plans de la collecte, de l'utilisation et de la divulgation des renseignements personnels.

Le principe de limitation est souvent remis en question dans le contexte de l'intelligence artificielle et des données massives. En effet, il semble difficilement cadrer avec le fonctionnement même de ces technologies, qui reposent sur une approche maximaliste de la collecte et de l'utilisation des données. Néanmoins, nous croyons que la minimisation du traitement de renseignements personnels demeure pertinente, à tout le moins dans une certaine mesure. En droit québécois, l'obligation d'adopter une approche minimaliste découle de trois principes : le principe de détermination des fins, le principe de limitation de la collecte et le principe de limitation de l'utilisation, de la communication et de la conservation. Pour des fins de clarté, les deux derniers principes seront regroupés en un seul : le principe de limitation qui s'appliquera à toutes les phases du traitement de renseignements personnels.

En vertu du principe de détermination des fins, une entreprise ou une organisation doit pouvoir déterminer la finalité pour laquelle un renseignement est traité[28]. Ce principe est souvent critiqué puisque dans le cadre de développement de SIA, il peut être très difficile de prévoir quelles seront les finalités de l'utilisation de renseignements personnels. Toutefois, bien que l'identification précise des fins poursuivies est un exercice complexe lorsque des techniques d'intelligence artificielle sont utilisées, des objectifs généraux devraient tout de même toujours pouvoir être formulés. Le principe de limitation prévoit quant à lui que seul le traitement de renseignements personnels pertinents en regard de ces fins peut être effectué[29]. Deux critères servent à déterminer la pertinence du traitement de renseignements personnels pour servir les fins déterminées. Il s'agit des critères de nécessité et de légitimité.

Le critère de nécessité dans un contexte d'IA

Le critère de nécessité se retrouve dans la *LPRPSP* que dans la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c A-2.1 (*Loi sur l'accès* ci-après). En vertu de ce critère, les renseignements personnels traités doivent être nécessaires pour atteindre les finalités identifiées en vertu du principe de détermination des fins. Or, la jurisprudence n'est pas constante quant à l'interprétation que doit recevoir le critère de nécessité[30]. Selon certaines décisions, le critère de nécessité n'est rempli que si une donnée est un renseignement qui « est indispensable, essentiel, et dont la présence "rend seule possible une fin ou un effet" »[31]. Dans un contexte d'intelligence artificielle et de données massives, cette interprétation est problématique. En effet, lorsque des techniques d'intelligence sont déployées, il peut en certains cas être difficile de prévoir à l'avance quelles variables permettront le mieux d'atteindre la fin visée. Ce n'est qu'à la fin du processus de

---

[28] *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1, articles 4 et 8. [LPRPSP]

[29] *Code civil du Québec*, RLRQ c CCQ-1991 à l'art 37. [C.c.Q]

[30] Cette question est traitée plus en détail dans : 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 » (2019) 465 *Développement récents en droit à la vie privée* 1 à la p 8.

[31] *M.L. c Gatineau (Ville de)*, 2010 QCCAI 68.

traitement de l'information qu'il devient possible d'identifier avec précision les données qui auront été nécessaires à l'atteinte des fins visées.

L'IA devient donc en quelque sorte, un outil de génération de nouvelles connaissances et de nouvelles hypothèses. Ce type de traitement de l'information permet de générer des connaissances qui pourraient avoir des effets bénéfiques pour l'ensemble de la population comme la médecine de précision. Une interprétation trop stricte du critère de nécessité pose un défi pour ce nouveau paradigme de recherche et constitue un frein à l'innovation. Une telle interprétation impose aussi un fardeau important aux entreprises qui exercent leurs activités en ligne. Cela est incompatible avec le juste équilibre qui doit être établi entre la vie privée des individus et les intérêts économiques des entreprises qui traitent des renseignements personnels.

Un second courant jurisprudentiel considère plutôt que le critère de nécessité est satisfait dès lors que les renseignements sont « nécessaires à l'objet du dossier en ce sens qu'ils ne sont pas superflus, sans objet ni pertinence. [Que] leur relation n'est pas gratuite ni fortuite »[32]. Cette interprétation est également problématique. En vertu de ce critère, une entreprise traitant des renseignements personnels aux fins d'offrir des contenus personnalisés pourrait justifier la nécessité de pratiquement n'importe quels renseignements. Le critère de nécessité comme moyen d'opérationnaliser les principes de limitations serait alors vidé de son sens.

Finalement, un dernier courant jurisprudentiel prévoit que le terme nécessité devrait recevoir une interprétation souple et dynamique s'appuyant sur un test en deux volets qui requiert d'évaluer si l'atteinte à la vie privée découlant du traitement d'un renseignement personnel est proportionnelle à l'importance de la finalité poursuivie. Cette interprétation est, elle aussi, insatisfaisante en contexte d'intelligence artificielle et de données massives puisqu'elle n'est pas suffisamment claire et aboutie. Elle laisse les entreprises et les organisations qui traitent des renseignements personnels dans une situation d'incertitude qui nuit tant à la protection de la vie privée qu'aux besoins des organisations.

Comme aucune des interprétations du critère de nécessité ne nous semble en mesure d'encadrer de manière satisfaisante le traitement de renseignements personnels dans un contexte d'intelligence artificielle et de données massives, nous recommandons de délaisser ce critère pour les situations faisant appel à l'IA et de plutôt opérationnaliser l'approche minimaliste du traitement des renseignements personnels en encadrant la légitimité des fins.

Le critère de licéité et la question des "fins acceptables"

Le critère de légitimité est déjà prévu par le droit québécois. Il requiert que toute entreprise ou organisation qui traite des renseignements personnels ait un intérêt

---

[32] *P.B c Lepage*, 2010 QCCQ 5982 au para 91.

légitime pour le faire[33] et que la collecte s'effectue de manière licite[34]. De plus, au niveau fédéral, la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5 prévoit déjà, au paragraphe 5(3) que toute forme de collecte, d'utilisation ou de communication de renseignements personnels doit viser des "fins qu'une personne raisonnable estimerait acceptables dans les circonstances". Bien que la proposition de la Commission énoncée au point 3 de son document de consultation est louable, il semble que toutes les formes de traitement qui seraient "inacceptables pour la société" ou qui pourraient se "révéler dangereuses pour la vie des personnes" seraient contraires aux exigences de la *LPRPSP* et de la *LPRPDE*. Ainsi, le critère de licéité qui anime l'application du principe de limitation sert déjà de rempart contre les traitements illégitimes ou motivés par des intentions malveillantes comme celles de tromper, de discriminer des personnes ou de leur causer du tort.

Toutefois, la signification des termes légitimes et illégitimes demeure évidement largement subjective. Ainsi, pour que le critère de licéité arrive à encadrer adéquatement le traitement de renseignements personnels, il devrait y avoir des indications plus claires quant à ce que constitue une finalité interdite. Définir ces finalités illégitimes est un exercice difficile, mais certains éléments de réponses, déjà avancés par différents acteurs au Canada et au Québec, doivent être considérés.

D'abord, le Commissariat à la vie privée (CPVP) du Canada a publié un document d'orientation pour l'application du paragraphe 5 (3) de la Loi sur la protection des renseignements personnels et les documents électroniques. Ces lignes directrices permettent d'identifier certains traitements de renseignements personnels qu'une personne raisonnable estimerait inacceptables dans les circonstances. Ces zones interdites ont été identifiées en s'appuyant sur des décisions judiciaires passées ainsi que sur une vaste consultation publique qui fut menée auprès de citoyens et d'intervenants canadiens[35]. Nous croyons qu'elles pourraient servir de guide pour interpréter le critère de légitimité prévu par le droit québécois à la protection des renseignements personnels. Ainsi, les traitements suivants devraient être considérés comme illégitimes et être proscrits :

1. Collecte, utilisation ou communication de renseignements personnels qui est autrement illégale ;
2. Collecte, utilisation ou communication à des fins qui causent ou sont susceptibles de causer un préjudice probable et grave à des individus (ex. : la lésion corporelle, l'humiliation, le dommage à la réputation ou aux relations, la perte financière, le vol d'identité, l'effet négatif sur le dossier de crédit, le dommage aux biens ou leur perte, et la perte de possibilités d'emploi ou d'occasions d'affaires ou d'activités professionnelles) ;

---

[33] C.c.Q, *supra* note 29, à l'art 37 ; *LPRPSP supra* note 29 à l'art 8.

[34] *LPRPSP*, *supra* note 29 à l'art 5.

[35] CPVP, *supra* note 5.

3. Publication de renseignements personnels dans le but de réclamer un paiement aux individus pour retirer ces renseignements ;
4. Obligation de communiquer le mot de passe des comptes de médias sociaux aux fins de la sélection des employés ;
5. Surveillance exercée par une organisation au moyen des fonctions audio ou vidéo de l'appareil de l'individu lui-même ;
6. Profilage ou catégorisation donnant lieu à un traitement injuste, contraire à l'éthique ou discriminatoire interdit en vertu de la législation sur les droits de la personne.

Aux six fins illégitimes identifiées par le CPVP devrait s'ajouter le traitement de données visant à réidentifier, sans nécessité autorisée ou apparente, des renseignements qui avaient été rendus non identifiables. Il nous apparaît préférable d'inscrire l'interdiction de réidentification dans le cadre de l'interdiction de traiter des renseignements personnels à des fins illégitimes plutôt que d'en faire une disposition à part entière qui serait difficile à faire appliquer concrètement[36].

Enfin, les travaux de la Déclaration de Montréal pour un développement responsable de l'IA pourraient également enrichir l'interprétation de ce qui doit être considéré comme étant des fins légitimes. Les principes de la déclaration découlent d'un exercice délibératif ayant rassemblé des citoyens, des professionnels et des universitaires d'horizons variés. Ils peuvent donc servir d'éclaireurs pour réfléchir aux pratiques qui bénéficient ou non de l'acceptabilité sociale :

- 2.2. Les SIA ne doivent pas être développés ni utilisés pour prescrire aux individus un mode de vie particulier, soit directement, soit indirectement en mettant en œuvre des mécanismes contraignants de surveillance, d'évaluation ou d'incitation.
- 2.3. Les institutions publiques ne doivent pas utiliser les SIA pour promouvoir ni défavoriser une conception de la vie bonne.
- 2.5. Les SIA ne doivent pas être développés pour propager des informations peu fiables, des mensonges et de la propagande et devraient être conçus dans le but d'en réduire la propagation.
- 3.8. Les SIA ne doivent pas être utilisés pour imiter ni modifier l'apparence physique, la voix et d'autres caractéristiques individuelles dans le but de nuire à la réputation d'une personne ou pour manipuler d'autres personnes.
- 7.4. Les SIA doivent éviter d'enfermer les individus dans un profil d'utilisateur ou une bulle filtrante, de fixer les identités personnelles

[36] Paul Ohm, « Broken Promise of privacy : responding to the surprising failure of anonymization » (2010) 57 UCLA Law Rev 1701 à la p 1758 ; Voir également *infra* section 5.

par le traitement des données de leurs activités passées et de réduire leurs options de développement personnel en particulier dans les domaines de l'éducation, de la justice et des pratiques commerciales.

- 7.5. Les SIA ne doivent pas être utilisés ni développés dans le but de limiter la liberté d'exprimer des idées et de communiquer des opinions dont la diversité est la condition de la vie démocratique[37].

En ce qui concerne la manière d'énoncer ces zones interditesde, nous considérons qu'elles devraient aussi être formulées dans des termes larges, à saveur constitutionnelle, et ayant une texture ouverte permettant de couvrir les limitations envisagées. Plusieurs approches peuvent être envisagées pour atteindre cet objectif, notamment :

- Une affirmation des droit des personnes sur qui portent les renseignements personnels qui serait énoncé à la manière d'un droit garanti par une charte (à l'opposée d'une interdiction). Ainsi, le texte pourrait affirmer le droit de chaque individu de ne pas voir ses données être collectées, traitées ou utilisées à des fins malveillantes, illégitimes, illégales ou préjudiciables ou encore le droit à la protection de chaque individu contre l'utilisation de ses données à de telles fins.
- Une interdiction générale de porter atteinte à un droit de l'individu, advenant que l'on reconnaisse un des droits ci-dessus, inspirée par exemple de l'interdiction de porter atteinte à la vie privée d'une personne du *Code civil du Québec*[38].
- Une interdiction plus limitative du type « *… sont interdits tout collecte, traitement ou utilisation des données d'une personne par les SIA, autre qu'à des fins de statistique, recherche, ou pour rendre un service sollicité par cette personne…* », par exemple.
- Une approche sectorielle est également envisageable et même souhaitable, pour renforcer la protection contre les débordements possibles de l'utilisation des SIA dans certains domaines, tels que la santé, les services financiers, l'éducation ou encore le développement de moyens de transport autonomes, et plus globalement les secteurs où le traitement de renseignements personnels peut avoir un impact important sur la vie des personnes. Ainsi, une interdiction plus large ou l'affirmation d'un droit général pourraient être tempérées par des dispositions plus spécifiques lorsque nécessaire.

Dans l'optique telle que posée, il faudrait également d'abord déterminer ce qu'est une limitation acceptable de l'utilisation des SIA. La simple interdiction de fins

---

[37] *Déclaration de Montréal pour un développement responsable de l'intelligence artificielle*, Montréal, 2018.

[38] C. c. Q *supra* note 29, art. 35.

illégitimes ou d'intentions malveillantes est-elle une limitation acceptable, ou pourrait-on établir la limitation acceptable au seuil de l'atteinte aux droits ou aux expectatives raisonnables d'une personne de ne pas subir de préjudice dû à l'application ou l'utilisation d'un SIA ? L'approche à privilégier en est-elle une de sanction du dommage, comme en droit civil, ou de la faute, à la manière du droit pénal ? La réponse à cette question pourrait varier selon le secteur et le domaine d'application selon que l'information traitée ou inférée par les SIA est d'ordre général et publique ou sensible et privée.

Il importe de spécifier qu'à notre avis, l'interdiction de traiter des renseignements personnels à des fins illégitimes devrait s'appliquer à tous les traitements de renseignements personnels et non pas uniquement aux traitements qui font appel à des systèmes informatisés ou à des SIA.

RECOMMANDATIONS RELATIVES AUX PRINCIPE #2 ET #3 DU DOCUMENT DE LA CAI

1. L'approche minimaliste en matière de traitement des renseignements personnels ne doit pas être abandonnée.

2. Le principe de détermination des fins ne doit pas être abandonné. Malgré le fait qu'il est difficile d'identifier les finalités précises de l'utilisation de renseignements personnels, les entreprises et les organisations qui traitent des données devraient être en mesure de formuler des objectifs généraux.

3. Le critère de nécessité comme moyen d'opérationnaliser l'approche minimaliste devrait être mis de côté au profit du critère de légitimité.

4. Certaines fins illégitimes devraient être identifiées pour l'application du critère de légitimité du traitement de renseignements personnels.

3. L'INDIVIDU EN CONTRÔLE : LES PRINCIPES DE CONSENTEMENT, D'ACCÈS À L'INFORMATION ET D'EXACTITUDE

Cette section aborde les principes 5, 6, 8, 9 et 10 du document de consultation de la Commission, qui portent sur les principes d'accès à l'information, d'explication, de révision et de rectification. Plus largement, nous nous intéressons à certains des principes des lois de protection des renseignements personnels qui entendent renforcer la capacité d'une personne à exercer un contrôle sur les modalités de circulation et de diffusion de ses renseignements personnels et qui s'inscrivent dans l'approche personnaliste des lois québécoises en matière de protection des renseignements personnels. Nous aborderons ainsi trois grands principes qui permettent

d'opérationnaliser ce contrôle individuel[39] : le principe de consentement et le droit d'opposition (3.1), le principe d'accès à l'information et le droit à l'explication (3.2) le principe d'exactitude des renseignements et le droit de révision (3.3). Comme nous le verrons, chacun de ces principes demande quelques ajustements pour demeurer en phase avec les réalités nouvelles qu'occasionne l'avènement de l'intelligence artificielle et des données massives.

L'idée qu'une personne puisse exercer un contrôle effectif sur ses renseignements personnels dans les environnements numériques contemporains fait l'objet de vives critiques. Le consentement semble plus ou moins bien adapté à la quantité et à la variété de traitements de renseignements personnels qui sont traités par des systèmes d'intelligence artificielle. De plus, l'opacité derrière les traitements de données, ainsi que l'utilisation de données pour des fins autres que celles pour lesquelles la personne a consenti (un traitement de renseignements personnels peut en cacher un autre), ou encore l'utilisation de données personnelles générées par des personnes qui ne connaissent même pas l'existence de ces données, rendent l'application efficace du consentement problématique.

Bien que nous reconnaissions que le numérique, l'intelligence artificielle et les données massives mettent à mal la capacité de l'individu à exercer un contrôle efficace sur ses renseignements, nous considérons toutefois qu'il ne faut pas complètement écarter la notion de contrôle des textes de loi. La capacité pour un individu de contrôler ses renseignements personnels assure le respect de l'autonomie individuelle et confère une légitimité au traitement de l'information. À notre avis, les principes permettant à l'individu d'exercer un contrôle sur ses renseignements personnels doivent conserver un rôle central en matière de protection des renseignements personnels.

3.1 Le principe de consentement et le droit d'opposition

En vertu du principe de consentement, à l'exception de certains cas particuliers prévus par la loi[40], un traitement de renseignements personnels n'est autorisé que si la personne concernée y a consenti. Pour consentir, la personne concernée doit être informée des finalités du traitement[41]. Au Québec, l'obtention du consentement manifeste de la personne est le principal critère de licéité du traitement de ses renseignements personnels. Or, puisque le principe de consentement soulève de difficiles questions aux plans de son efficacité et de la forme qu'il doit prendre, il est raisonnable de s'interroger sur la pertinence de prévoir des circonstances où d'autres critères pourraient être utilisés pour légitimer le traitement de renseignements

[39] C.c.Q, supra note 29 aux arts. 35 à 41.

[40] Les dispositions qui permettent de traiter des renseignements personnels sans consentement sont de divers ordres. Par exemple, il peut être possible de traiter des RP sans consentement à des fins de recherche (*LPRPSP* art 21 ; *Loi sur l'accès* art 59), à des fins de répressions du crime (*Loi sur l'accès* art 41.2 ; *LPRPSP* art 18(3)), à des fins de prospection commerciale ou philanthropique (*LPRPSP* art 23) ou lorsque le traitement réalisé est manifestement dans l'intérêt de la personne, mais que celle-ci ne peut pas consentir en temps opportun (*LPRPSP* art. 6). C'est le cas par exemple d'une situation médicale urgente (Loi sur l'accès art 59 (4))

[41] *LPRPSP supra* note 29 à l'art 14 ; *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c A-2.1, art 65. [*Loi sur l'accès*]

personnels. Toutefois, cette perspective ouvre également une réflexion plus large sur la définition de ces critères alternatifs et l'identification de ces circonstances. Dans son document de consultation, la Commission semble plus particulièrement s'intéresser à la pertinence et l'efficacité du consentement dans un contexte de profilage, d'analyse ou de prédiction – que nous avons assimilé plus tôt à la notion de traitements de renseignements personnels à haut risque – c'est donc sur ce contexte particulier que notre propos portera.

Puisque les lois québécoises de protection des renseignements personnels prévoient déjà une obligation d'obtenir le consentement manifeste des personnes, il n'est pas à notre avis nécessaire de prévoir une nouvelle obligation d'information pour les entreprises ou les organismes qui ont recours à des techniques de profilage, d'analyse, de prédiction, d'inférence ou de prise de décision automatisée. Toutefois, des dispositions prévoyant que les modalités de consentement doivent être modulées en fonction des risques que comportent certains traitements de renseignements personnels seraient intéressantes. Dans le cadre de traitements de renseignements personnels qui comportent des risques importants pour les droits fondamentaux, notamment le droit à la vie privée ou le droit à l'égalité, nous croyons que les organisations et les entreprises devraient avoir l'obligation d'obtenir un consentement explicite. La configuration par défaut du mode de traitement de l'information devrait alors adopter une logique de « opt-in ».

À l'exception de la surveillance systématique à grande échelle de zones accessibles au public, pour lequel cela n'est pas possible d'un point de vue pratique, les organismes et les entreprises qui mettent en oeuvre des traitements de renseignements personnels à haut risque devraient obtenir un consentement explicite pour mettre en œuvre de tels traitements. Dans les cas où l'obtention du consentement pose problème, une autorisation de la CAI pourrait aussi permettre de mettre en oeuvre des traitements de renseignements personnels à haut risque.

Pour ce faire, l'entreprise ou l'organisme devrait présenter une demande d'autorisation écrite à la Commission dans laquelle il fait la démonstration que le traitement qu'il souhaite entreprendre est nécessaire :

- à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
- à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
- aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des

> données à caractère personnel, notamment lorsque la personne concernée est un enfant[42]

Par ailleurs, lorsque le traitement est réalisé à des fins d'étude, de recherche ou de statistique en milieu universitaire, la Commission pourrait déléguer son pouvoir d'autorisation aux comités d'éthique à la recherche des universités qui évaluent déjà les risques associés aux projets de recherche traitant des renseignements personnels. Cette délégation du pouvoir d'autoriser l'utilisation de renseignements personnels sans consentement dans le contexte de recherche académique permettrait de simplifier le long et complexe processus auxquels les chercheurs sont confrontés les chercheurs pour l'instant. Cela permettrait également de rétablir un certain équilibre avec le reste du Canada où les procédures sont moins contraignantes. Cet allègement des procédures devrait s'appliquer à tous les traitements de renseignements personnels pour des fins de recherche et non pas uniquement aux traitements à haut risque.

Par ailleurs, en ce qui a trait aux traitements à plus faibles risques, notamment le traitement de données dépersonnalisées, ceux-ci pourraient faire l'objet d'allégements en matière de consentement. Par exemple, la réutilisation de données à de nouvelles fins par l'entreprise ou l'organisme qui les a collectées pourrait être réalisée sans obtenir un nouveau consentement dans les cas où les données ont été rendues non-identifiables. En d'autres mots, il semble pertinent de repenser les conditions de licéité du traitement des renseignements personnels en identifiant des fondements juridiques autres que le consentement qui permettrait de justifier le traitement des renseignements personnels. L'intérêt public et l'intérêt légitime du responsable de traitement prévus à l'article 6 e) et f) du *RGPD* nous semblent des fondements alternatifs qui devrait être considéré par la Commission.

Enfin, il importe de rappeler que le principe de consentement est corollaire au droit d'opposition. L'obtention du consentement est dénuée de valeur si l'individu faisant l'objet d'un traitement de renseignements personnels n'a pas de possibilité réelle de refuser. Ainsi, à l'exclusion des cas d'exceptions au consentement, un individu devrait toujours être en mesure de s'opposer à un traitement de renseignements personnels. Cela est déjà implicitement prévu tant dans la *Loi sur l'accès* que dans la LPRPSP. Toutefois, bien que déjà existant, ce droit d'opposition mériterait d'être énoncé de manière plus explicite.

Pour ce faire, il serait intéressant de s'inspirer du droit de ne pas faire l'objet d'une décision fondée sur un traitement automatisé des données. On retrouve par exemple ce principe à l'article 22 du RGPD.

> **ARTICLE 22 DU *RGPD* - 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

[42] RGPD, *supra* note 5, art 6.

> effets juridiques la concernant ou l'affectant de manière significative de façon similaire […] »

Ce droit de ne pas faire l'objet d'une forme de traitement de renseignements personnels donnés pourrait aussi viser plus large et s'appliquer à tous les traitements de renseignements personnels à haut risque, ou à toute forme de traitement de renseignements personnels dont la licéité s'appuie non pas sur le consentement mais plutôt sur les "intérêts légitimes poursuivis par le responsable du traitement".

Une telle chose est prévue à l'article 21 du *RGPD* qui permet à la personne dont les renseignements personnels font l'objet d'un traitement justifié par le biais du point f) de l'article 6 de refuser que ses renseignements fassent l'objet d'un tel traitement. L'article 21 précise d'ailleurs que ce droit d'opposition s'applique dans les cas où le traitement vise des fins de profilage. Lorsque la personne se prévaut de son droit d'opposition, le responsable du traitement doit cesser d'exploiter les données, sauf s'il réussit à démontrer que des « motifs légitimes et impérieux (…) prévalent sur les intérêts et les droits et libertés de la personne ». Or, la jurisprudence européenne relative au droit d'opposition enseigne aussi que le droit à la protection des données à caractère, qui est un droit fondamental de la personne[43], devra généralement prévaloir sur l'intérêt économique d'une entité qui traite ces données.[44] Par conséquent, une entreprise qui exploite des renseignements personnels ne pourra faire valoir un motif financier pour s'opposer à l'exercice du droit d'opposition d'une personne.

Cette nuance illustre bien pourquoi il est important d'ancrer la protection des renseignements personnels dans une perspective plus large de protection des droits et libertés de la personne. Ainsi, selon nous, si la Commission en venait à envisager l'introduction de fondements juridiques supplémentaires, qui permettraient entre autres de justifier le traitement de renseignements personnels sans avoir préalablement obtenu le consentement de la personne, elle devrait aussi étudier la possibilité d'introduire un droit d'opposition et adopter une approche qui reconnaît explicitement la protection des renseignements personnels comme un droit fondamental de la personne.[45] Dans de telles conditions, la création d'un modèle hybride, où le consentement ne serait pas le seul fondement permettant de justifier le traitement de renseignements personnels, notamment à des fins de profilage, peut être envisagée. Cependant, si le consentement devait rester comme condition nécessaire au traitement légitime des données, il devrait être renforcé au moment de la collecte par une procédure d'« *opt-in* » par laquelle la personne doit explicitement consentir au traitement de ses renseignements personnels.

---

[43] Le droit à la protection des données à caractère personnel est protégé par l'article 8 de la *Charte des droits fondamentaux de l'Union européenne*.

[44] *Google Spain SL c. Agencia Española de Protección de Datos (AEPD)*, ECLI:EU:C:2014:317 au paragraphe 97.

[45] Il s'agit par ailleurs d'une des propositions soumises par le CPVP au point 2 de son document de consultation, *supra* note 5.

Ceci dit, il ne s'agit pas de faire un copié/collé des dispositions européennes puisque celles-ci ne sont pas satisfaisantes à certains égards. Par exemple, en ce qui a trait à l'article 22, il conviendrait de garder la structure du droit de ne pas faire l'objet d'une décision fondée sur un traitement automatisé sans pour autant limiter ce dernier à la nécessité que cette décision produit des effets juridiques ou affecte la personne de manière similaire. En effet, il est important de garder à l'esprit que les effets produits par une décision automatisée peuvent avoir des conséquences importantes sur la vie des personnes sans pour autant que l'affectation provienne d'effets juridiques ou d'effets « similaires ». Ainsi, il serait utile d'étendre les « effets » à des effets affectant la personne de manière significative qu'ils soient juridiques ou non, ou même d'éliminer ce concept d'« effets » et donc d'élargir la portée du droit à toute décision fondée sur un traitement automatisé.

3.2 Le principe d'accès à l'information : vers un droit à l'explication ?

Un autre principe fondamental permettant l'opérationnalisation du contrôle de l'individu sur ses renseignements personnels est le principe d'accès à l'information. Outre quelques situations qui peuvent faire obstacle au droit d'accès[46], toute personne qui le demande doit pouvoir avoir accès gratuitement à tous les renseignements personnels qu'une entreprise ou une organisation possède à son sujet[47].

En vertu de l'article 84 de *la Loi sur l'accès*, un renseignement informatisé doit être communiqué sous la forme d'une transcription écrite et intelligible. Alors que l'article 84.1 de cette même loi prévoit quant à lui qu'en certaines circonstances l'assistance d'un professionnel peut être demandée par une personne qui désire de l'aide pour comprendre les renseignements auxquels on lui donne accès. Ces dispositions prennent un nouveau sens dans un contexte de recours à l'intelligence artificielle. En effet, nous croyons qu'elles ouvrent la porte à la mise en place d'un droit à l'explication des traitements des renseignements personnels fondés sur un traitement automatisé.

Il importe toutefois de rappeler que l'interprétabilité des SIA en est encore à ses balbutiements et qu'il s'avère difficile en pratique de donner une explication claire et limpide du « raisonnement des algorithmes ». Cela dit, nous croyons que les lois québécoises devraient tout de même prévoir un droit de recevoir une explication, garantie par un professionnel, de la logique sur laquelle un traitement automatisé est fondé, de la liste de renseignements ayant nourri l'algorithme et, dans la mesure du possible, une explication des facteurs et des paramètres les plus importants ayant mené à la prise d'une décision. Par ailleurs, nous considérons aussi que le devoir d'information des responsables ou des opérateurs de SIA devrait aller plus loin. En effet, en plus de ce qui est prévu, les responsables du traitement devraient informer de l'existence d'un droit d'accès, de retrait, de révision et de rectification pour renforcer

[46] C.c.Q, *supra* note 29, art. 39.

[47] Art. 27 et 33 *LPRPSP supra* note 28, et art. 9 et 11 Loi sur l'accès, *supra* note 41.

cette transparence. Ce devoir d'informer est d'autant plus important lorsque le SIA sert à la prise de décision, et ce, tant par une administration publique que par des acteurs privés. C'est ce que nous abordons à la prochaine sous-section.

3.3 Le principe d'exactitude : le droit à la révision d'une décision automatisée et le droit à la rectification

En vertu du principe d'exactitude, les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés. Deux mécanismes permettent l'application de ce principe. D'abord, le Québec bénéficie d'une certaine forme de ce que l'Union européenne appelle le droit à l'effacement[48]. En effet, une personne peut demander à ce que soit supprimé un renseignement personnel à son égard si ce dernier est périmé, s'il n'est pas pertinent en regard des fins pour lesquelles il a été collecté ou si la collecte n'était pas autorisée par la loi[49]. Comme mentionné à la section portant sur les enjeux définitionnels, les inférences, les profils et le résultat de décisions automatisées doivent être considérés comme des renseignements personnels. Ainsi, si ceux-ci sont périmés ou s'ils ont été collectés de manière illicite, la personne concernée peut demander à ce qu'ils soient supprimés.

Par ailleurs, en vertu du principe d'exactitude, il est aussi possible de faire rectifier un renseignement inexact, incomplet ou équivoque[50]. Or dans le contexte d'inférences, de profils ou de décisions automatisées, il peut s'avérer difficile de tenir un débat sur l'exactitude d'un résultat. Surtout lorsque le SIA ayant produit le renseignement se montre indéchiffrable pour l'humain. Ainsi, nous croyons que lorsqu'une mésentente survient quant à l'exactitude d'un renseignement ayant fait l'objet d'un traitement automatisé, le droit à la rectification ne devrait pas s'appliquer. Les solutions pour répondre à de telles situations devraient plutôt être la révision par un être humain ou la suppression du renseignement. Le choix de la solution devrait revenir à la personne ayant soulevé le caractère inexact des renseignements.

Ainsi, nous considérons que le droit à la révision d'une décision prise par un système d'intelligence artificielle devrait exister, mais peut-être pas sous la forme proposée dans le document de consultation. Il devrait s'agir d'un droit complémentaire au droit d'opposition qui s'appliquerait lorsqu'une personne ne peut faire valoir son droit principal d'opposition ou dans les cas où la décision serait erronée ou déraisonnable.

Dans ces cas, le responsable de traitement devrait être contraint, si la personne l'exige, à faire réviser par une personne physique la décision prise initialement par un SIA. Enfin, pour que ce régime soit efficace, il serait préférable de *renverser le fardeau de la preuve* lorsqu'un outil d'IA est utilisé. Cela signifie que ce n'est pas à la personne concernée de prouver qu'elle a fait l'objet d'une décision fondée sur un traitement

---

[48] RGPD, *supra* note 5, art. 17.

[49] C.c.Q, *supra* note 29, art 40 ; *LPRPSP, supra* note 28, art 28. ; *Loi sur l'accès, supra* note 41, art. 128.

[50] C.c.Q, *supra* note 29, art 40.

automatisé ou que cette décision produit des effets dommageables à son encontre. Au contraire, c'est au responsable de traitement de prouver que le demandeur n'a pas fait l'objet d'une décision fondée sur un traitement automatisé et que son droit est respecté ou de prouver que cette décision ne produit pas d'effets dommageables. Cette proposition s'inspire du régime qui prévaut en Europe en vertu de l'article 22 du *RGPD.*

RECOMMANDATIONS RELATIVES AUX PRINCIPES # 5, 6, 8, 9 ET 10 DU DOCUMENT DE LA CAI
1. L'importance de la capacité d'un individu à exercer un contrôle sur les modalités de circulation et de diffusion de ses renseignements personnels devrait être réaffirmée ;
2. Les traitements de renseignements personnels à haut risque devraient faire l'objet d'un consentement explicite et adopter une logique « opt-in » ou bénéficier d'une autorisation écrite de la Commission pour être autorisés ;
3. Les données rendues non identifiables devraient pouvoir être réutilisées sans nouveau consentement par l'organisation ou l'entreprise les ayant collectées initialement ;
4. Un droit de refuser de faire l'objet d'un traitement de renseignements personnels à haut risque devrait être prévu explicitement ;
5. Un droit de recevoir une explication, garantie par un professionnel, de la logique sur laquelle une prédiction ou une décision automatisée est fondée et dans la mesure du possible, une explication des facteurs et des paramètres les plus importants ayant mené à la prise d'une décision devrait être prévu.
6. Le droit à la suppression des renseignements personnels devrait s'appliquer aux inférences, profils et résultats de décisions automatisées.
7. Les renseignements personnels ayant fait l'objet d'un traitement automatisé qui sont inexacts, incomplets ou équivoques doivent pouvoir être révisés par un être humain ou supprimés.

4. PRINCIPES DE RESPONSABILITÉ DÉMONTRABLE ET DE TRANSPARENCE

Cette section aborde les principes 7, 11, 12, 13, 14 15, 16 et 17 du document de consultation de la CAI qui porte, de manière générale, sur la responsabilité et la

l'imputabilité des entreprises qui traitent des renseignements personnels. Le principe de responsabilité veut qu'une organisation ou une entreprise soit responsable des renseignements personnels qui sont sous son contrôle. Elle doit donc s'assurer d'agir conformément aux obligations légales associées au traitement de ces renseignements. Le principe de transparence nourrit le principe de responsabilité, puisqu'il permet de mettre en lumière les mesures prises par les responsables de traitement pour respecter les obligations qui leur incombent. Cela permet aussi de mettre en lumière d'éventuels écarts aux obligations.

Le principe de transparence se décline en *deux volets :*

- Le volet *individuel*, dont nous avons traité au titre précédent avec les principes de détermination des fins, de consentement et d'accès à l'information;
- Et un volet *global, systémique et sociétal*. Ce volet plus global de la transparence requiert que les entreprises et les organisations fassent preuve de transparence non pas uniquement à l'égard des individus, mais également à l'égard d'institutions publiques qui représentent et agissent au nom de ceux-ci. Cette transparence systémique et sociétale contribue à nourrir la confiance de la population et pallier les asymétries de pouvoir qui marquent les interactions entre les entreprises, les organisations et les individus.

Selon nous, la Commission d'accès à l'information est l'institution qui doit être responsable d'assurer la transparence systémique en matière de protection des renseignements personnels. En plus de ses pouvoirs actuels, elle pourrait être chargée de conseiller et contrôler les organisations qui conduisent des évaluations des risques relatifs à la protection des renseignements personnels (EFVP) et des évaluations de l'incidence algorithmique (EIA). Elle pourrait aussi être chargée de réaliser des audits ou d'accorder des autorisations préalables à la mise en oeuvre de traitements de renseignements personnels à haut risque.

4.1 Les outils d'évaluations d'impacts relatifs à la protection des données

De telles évaluations devraient être obligatoires pour les organismes et les entreprises qui traitent des renseignements à haut risque. En effet, les organismes et les entreprises qui réalisent des traitements de renseignements personnels à haut risque devraient tous soumettre leurs activités à une évaluation des facteurs relatifs à la vie privée. De plus, les organismes et les entreprises qui réalisent des traitements *automatisés* de renseignements personnels à haut risque devraient, en plus de l'évaluation de EFVP, soumettre leurs activités à une évaluation de l'incidence algorithmique.

Ces deux types d'impacts relatifs à la protection des données devraient permettre de déterminer le niveau de risque d'un traitement afin de déterminer les mesures à prendre pour mitiger les éventuels impacts négatifs sur les droits fondamentaux des

individus. L'outil d'évaluation de l'incidence algorithmique du gouvernement du Canada et le logiciel PIA de la Commission nationale de l'informatique et des libertés (CNIL) constituent des modèles intéressants d'outils pour réaliser des évaluations d'impacts relatifs à la protection des données.[51] Développé dans le cadre de la *Directive sur la prise de décision automatisée*[52], l'outil d'évaluation de l'incidence algorithmique vise à aider les institutions à mieux comprendre et atténuer les risques associés aux systèmes de prise de décision automatisés en fournissant les exigences appropriées en matière de gouvernance, de surveillance, de rapport et d'audit[53].

Pour réaliser l'évaluation de l'incidence algorithmique, une organisation qui développe un système décisionnel automatisé doit répondre à 60 questions sur une interface web. Après avoir rempli le questionnaire, l'organisation reçoit un score qui représente le risque associé au déploiement de son SIA. Selon le score qu'elle reçoit, l'organisation doit se plier à un certain nombre de mesures. Par exemple, les systèmes de prise de décision qui sont classés dans la catégorie niveau d'incidence IV, doivent faire l'objet d'une évaluation par au moins deux experts qualifiés et obtenir une approbation préalable à l'exploitation de la part du Conseil du trésor[54]. Il pourrait aussi être utile d'inclure des normes de sécurité qui ne figurent pas explicitement dans la loi comme, par exemple, des processus de certification à la norme ISO 27701 relative au management de la vie privée et d'exiger ce type de certification au stade de l'EFVP afin de garantir un niveau de sécurité supérieur.

La Commission devrait, selon nous, réfléchir à de tels outils adaptés à sa réalité.

L'évaluation incidence algorithmique de la Commission devrait notamment traiter des mesures prises pour détecter les biais dans les données, pour assurer la représentativité des données en fonction de l'objectif, pour mitiger les risques d'erreurs et de biais des prédictions et assurer la qualité et la précision des prédictions. L'EIA devrait prendre en compte la fin poursuivie par le responsable du traitement de données : l'entreprise privée se sert de données générées avec des fonds publics (en santé par exemple) pour entraîner des SIA qui seront revendus, souvent à ce même système public pourrait être considéré comme un facteur militant en faveur d'un niveau de risque plus élevé.

Les traitements de renseignements personnels qui seraient considérés comme ayant les plus hauts risques en vertu de ces outils pourraient être contraints d'obtenir une approbation préalable octroyée par la CAI ou encore être obligés de faire l'objet d'un

---

[51] Gouvernement du Canada, Évaluation de l'Incidence Algorithmique, en ligne : <https://ouvert.canada.ca/aia-eia-js/?lang=fr > ; France, Commission Nationale de l'informatique et des liberté, « Outil PIA : téléchargez et installez le logiciel de la CNIL», en ligne : <https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil>

[52] Gouvernement du Canada, Conseil du Trésor, *Directive sur la prise de décision automatisée*, Ottawa, 2019, en ligne : <https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32592#appA>

[53] Noel Corriveau et Michael Karlin, *L'Évaluation d'impact algorithmique du gouvernement du Canada: Un deuxième essai*, en ligne :https://medium.com/@supergovernance/l%C3%A9valuation-d-impact-algorithmique-du-gouvernement-du-canada-un-deuxi%C3%A8me-essai-e7578cf9cdee

[54] *Directive sur la prise de décision automatisée, supra* note 52, à l'annexe C

audit annuel. Dans le cadre de ces pouvoirs, la CAI devrait pouvoir avoir accès non seulement aux codes sources des algorithmes, mais également aux données qui les ont entraînées. Autrement, les codes sources des algorithmes ont peu de valeur.

4.2 Les cadres de gouvernance

Les lois québécoises de protection des renseignements personnels devraient prévoir l'obligation, pour les entreprises et les organisations qui traitent des renseignements personnels, d'adopter et de rendre public un cadre de gouvernance de la protection des renseignements personnels. Cette obligation a une double vocation. D'abord, elle permet à l'individu d'avoir une compréhension plus approfondie de la manière dont sont traités ses renseignements personnels et, ensuite, elle permet à la commission d'exercer son pouvoir de surveillance plus aisément. Le fait d'obliger les responsables de traitement de renseignements personnels à rendre aisément accessibles leurs pratiques et politiques concernant la gestion des renseignements personnels permettrait de vérifier plus facilement si les entreprises agissent en conformité avec leurs obligations légales.

Les cadres de gouvernance des renseignements personnels devraient notamment comprendre les éléments suivants :

- **Identification de la chaîne humaine des responsabilités** : Les entreprises et les organisations qui traitent des renseignements personnels devraient être dans l'obligation d'identifier tous les responsables qui interviennent au cours d'un traitement de renseignements personnels. Cette approche globale prenant en contre l'ensemble du cycle de vie d'un traitement de renseignements personnels s'inspire du processus de certification de la FDA concernant les Artificial Intelligence and Machine Learning Software as a Medical Device[55]. Cela permet de mettre en place une boucle vertueuse qui encourage l'adoption d'une démarche de qualité et qui permet d'identifier les failles plus aisément.

- **Traçabilité des renseignements personnels:** Les entreprises et les organisations qui traitent des renseignements personnels devraient rendre publique la provenance de leurs données et indiquer s'ils les communiquent à d'autres organisations. Cette traçabilité permet de faire porter la responsabilité des obligations en matière de protection des renseignements personnels à l'ensemble des organisations par lesquelles ils passent.

- **Fuite de données:** Les procédures en place pour prévenir les fuites de données ainsi que celles visant à informer les utilisateurs en cas de fuite ou vol des données devraient être prévues au cadre de gouvernance des

[55] U.S Food and Drug Administration, *Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) - Discussion Paper and Request for Feedback*, en ligne: https://www.fda.gov/files/medical%20devices/published/US-FDA-Artificial-Intelligence-and-Machine-Learning-Discussion-Paper.pdf

renseignements personnels. Par ailleurs, les incidents de sécurité liés à l'utilisation d'un SIA et impliquant des renseignements personnels devraient être divulguée non seulement aux autorités concernées mais également aux personnes concernées et au public. Ces individus, sujets du traitement des renseignements personnels, touchés par un incident de sécurité, et le public, surtout dans une optique de données massives, ont certainement l'intérêt nécessaire et le droit d'être avisés des incidents de sécurité. Cette recommandation constitue un élargissement du principe 15 de la Comission.

- **Minimisation des données** : Bien que le critère de nécessité doive être mis de côté. L'approche minimaliste en matière de traitements des renseignements personnels doit subsister. Les entreprises et les organisations devraient justifier dans leur cadre de gouvernance la pertinence des renseignements qu'ils traitent.

  Des métriques mathématiques telles que la précision de la prévision (f1 compte), le taux d'erreur, la mitigation des biais pourraient être utilisées pour justifier l'importance d'un renseignement. Par exemple, le traitement d'un renseignement pourrait être justifié en démontrant que l'ajout de cette donnée a un impact positif sur ces métriques. Une analyse pondérant les risques et les bénéfices d'un traitement pourrait également servir de justification. L'opportunité de recourir ou non à des données rendues non identifiables ou à des données synthétiques devrait aussi être discutée dans cette section. Une entreprise ou une organisation devrait justifier pourquoi elle a recours à des renseignements personnels identificatoires.

  Une justification valable pour traiter des renseignements personnels identificatoires serait par exemple le fait que, dans le domaine de la santé, certains renseignements doivent demeurer identifiables pour apparier des jeux de données utilisés.Dans le domaine de la santé toujours, on pourrait justifier le fait de ne pas recourir à des données synthétiques par l'impossibilité. En effet, l'usage de renseignements synthétiques dans ce domaine ne peut généralement pas être envisagé puisqu'il n'est pas possible de synthétiser les données requises. Par exemple, il n'est pas possible de synthétiser une tumeur cancéreuse sans avoir recours à de vraies tumeurs.

- **Privacy by design:** Le principe de vie privée dès la conception est important. Il suppose de mettre en place des mesures organisationnelles visant à assurer la protection de la vie privée dès le début des projets. Or, de l'avis de certains, ce principe est trop flou pour produire des effets légaux opérants. Une mesure mitoyenne nous apparaît être de prévoir une obligation pour les organisations et les entreprises de justifier leurs choix et leurs actions en matière de vie privée à la lumière du principe privacy by design dans leur cadre de gouvernance des renseignements personnels.

4.3. Le principe de responsabilité

Les évaluations d'impacts relatifs à la protection des données avant qu'une entreprise ou un organisme amorce le traitement de renseignements personnels permettent d'anticiper et de prévenir des atteintes au droit à la protection des renseignements personnels en amont. Les cadres de gouvernance de données permettent à la commission d'accès à l'information d'intervenir plus efficacement dans le cadre de son pouvoir de surveillance. Or pour s'assurer que les entreprises et les organisations respectent véritablement le principe de responsabilité, ces mesures doivent s'accompagner d'autres mécanismes qui permettent à la Commission de faire respecter la loi. Cela inclut notamment des pouvoirs de sanctions. Tous les acteurs qui font partie de la chaîne humaine de responsabilité d'un traitement de renseignements personnels, c'est-à-dire tous les acteurs qui sont intervenus à l'une ou l'autre des étapes du traitement de renseignements personnels, doivent pouvoir être sanctionnés par la Commission. Les pénalités devraient être suffisamment importantes pour être prises au sérieux par les géants du numérique sans être inéquitables pour les plus petits joueurs. Pour répondre à ces impératifs, les amendes fixées en fonction du chiffre d'affaires annuel mondial de l'entreprise ou de l'organisme semblent être l'option la plus appropriée. C'est d'ailleurs l'approche retenue par l'Union européenne dans le cadre du RGPD[56].

Recommandations relatives aux principes *# 7, 11, 12, 13, 14, 15, 16 et 17* du document de la CAI

1. Les traitements de renseignements personnels à haut risque devraient faire l'objet d'évaluation d'impacts relatifs à la protection des données.

2. La Commission devrait réfléchir à mettre en place un outil d'évaluation d'impacts relatifs à la protection des renseignements personnels en ligne.

3. Les entreprises et les organisations qui traitent des renseignements personnels devraient avoir l'obligation d'adopter et de rendre accessible publiquement un cadre de gouvernance des données.

4. Les pénalités pour manquements aux obligations en matière de protection des renseignements personnels devraient être fixées en fonction du chiffre d'affaires annuel mondial des entreprises fautives.

[56] RGPD, *supra* note 5, art 83.

5. LES QUESTIONS SPÉCIFIQUES

Dans son document de consultation, la Commission formule plusieurs questions plus spécifiques. L'objectif de cette section est d'apporter certains éléments de réponse à ces questions.

- **EST-CE QUE L'UTILISATION DE DONNÉES ANONYMISÉES OU DE JEUX DE DONNÉES SYNTHÉTIQUES POUR L'ENTRAÎNEMENT DES SIA DEVRAIT ÊTRE FAVORISÉE ?**
    - La question telle que posée suppose une réponse évidemment positive d'un point de vue sociojuridique. Lorsque techniquement possible, il est clairement préférable d'avoir recours à des données synthétiques et à des données anonymisées. L'utilisation de données synthétiques est d'ailleurs identifiée comme une approche technique particulièrement intéressante permettant de remédier aux contraintes liées au respect de la vie privée, en plus de proposer des avantages intrinsèques, comme la possibilité de simuler des scénarios autrement difficilement observables ou reproductibles[57]. Toutefois il importe de réitérer que dans le domaine de la santé, l'usage de renseignements synthétiques ne peut généralement pas être envisagé puisqu'il n'est pas possible de synthétiser les données requises. Par exemple, il n'est pas possible de synthétiser une tumeur cancéreuse sans avoir recours à de vraies tumeur
    - L'usage de données anonymisées est également souhaitable. Une utilisation plus répandue de données anonymisées contribuerait à améliorer la confiance du public dans les SIA en posant un obstacle additionnel aux violations possibles de la vie privée ou de la confidentialité de données personnelles. Cependant, l'anonymisation des données n'est pas une panacée pour régler les problèmes liés à la protection des individus face aux SIA. Selon une étude parue dans *Nature Communications*, les données anonymisées peuvent presque toujours être réidentifiées[58].Dans l'attente d'une solution technique qui pourrait éventuellement rendre la réidentification plus complexe, voire impossible, nous considérons tout de même que l'anonymisation des données contribue au développement d'un environnement plus sain pour la propagation des SIA.
- **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 ?**
    - Encore une fois, on se heurte ici à des problèmes de réalisme dans l'application d'une telle règle venant sanctionner ces pratiques. On peut être tenté de sanctionner les abus en matière de réidentification de données préalablement

[57] OCDE, *L'intelligence artificielle dans la société*, Éditions OCDE, 2019, Partis p. 114 et 119, en ligne : https://doi.org/10.1787/b7f8cd16-fr.

[58] LUC ROCHER, JULIEN M HENDRICKX ET YVES-ALEXANDRE DE MONTJOYE, « Estimating the success of re-identifications in incomplete datasets using generative models» (2019) 10 *Nature Communications* 3069, en ligne : https://doi.org/10.1038/s41467-019-10933-3.

dépersonnalisées ou désidentifiées puisque l'on sait qu'il y a toujours une possibilité pour les opérateurs de revenir en arrière bien que les données aient fait l'objet d'une procédure de désidentification. Mais comment opérer le contrôle d'une telle règle ? Il apparaît compliqué en termes de moyens de contrôler (même avec des audits fréquents) ce genre de pratiques. Il semble plus opportun de déployer des efforts soutenus sur la sécurité des renseignements personnels détenus par un responsable de traitement pour assurer une protection optimale. Cela n'empêcherait pas, par ailleurs, d'interdire des pratiques qui sont difficiles à contrôler.

- Une telle interdiction pourrait notamment s'avérer utile dans des cas où il y aurait échange de données déidentifiées entre différentes parties. Une partie de la chaine de traitement des données n'ayant initialement pas eu accès aux données préalablement à la dépersonnalisation pourrait alors être plus aisément identifiable et sanctionnable, sous réserve des considérations techniques que cela pose.

- **D'APRÈS VOUS, QUELLES SONT LES MEILLEURES SOLUTIONS POUR RÉSOUDRE LES TENSIONS ENTRE LA RECHERCHE ET LE DÉVELOPPEMENT DES SIA ? QUELLES CONDITIONS DEVRAIENT ENCADRER CES SOLUTIONS ? EST-CE QUE D'AUTRES PISTES DE SOLUTION DEVRAIENT FAIRE PARTIE DE LA RÉFLEXION DE LA COMMISSION ?**

  - Les principes d'éthique devraient être mis de l'avant et tous les acteurs devraient y adhérer. Il semble déjà se former un certain consensus quant à certains de ces principes régulateurs du domaine de l'intelligence artificielle. L'article «Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI» du *Berkman Klein Center for Internet & Society at Harvard University*[59] est d'ailleurs fort intéressant à ce sujet. Une étude comparative y est faite de trente-six documents de premiers plans établissant des principes de l'intelligence artificielle, incluant la *Déclaration de Montréal,* le Plan coordonné dans le domaine de l'intelligence artificielle de la Commission européenne, et les documents sur les principes de l'intelligence artificielle proposés respectivement par l'OCDE, le G20, Google, Microsoft, et plusieurs autres. Huit thèmes principaux en ressortent, dont la plupart sont abordés dans le Document de consultation de la Commission, mais certains gagneraient à être davantage mis de l'avant et la Commission est encouragée à s'en inspirer.

  - Pour répondre à la question posée, il faudrait donc soumettre la recherche à des politiques et à des comités d'éthique y compris dans le cadre de projets financés par le secteur privé et impliquant des universités.

[59] Jessica Fjeld et al., « Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI» (2020) *Berkman Klein Center Research Publication*, en ligne : <https://ssrn.com/abstract=3518482> ou http://dx.doi.org/10.2139/ssrn.351848.

- Certains acteurs appréhendent toute tentative de réglementer l'intelligence artificielle, prétendant qu'il s'agit d'un obstacle à l'innovation dans le domaine. Or, il faut cesser de croire que l'innovation est une fin en soi et reconsidérer le mythe de la machine. Comme toute innovation et toute technologie, les SIA ont besoin d'être réglementés et encadrés. Ce faisant, la confiance du public en serait améliorée et l'innovation en bénéficierait grandement. À l'opposé, une liberté absolue du type *free-for-all* crée un environnement d'innovation malsain, où les dérapages sont faciles et où le respect des droits individuels est relégué au second plan. C'est également ce qui exacerbe les tensions entre les différents acteurs. Une approche impliquant un maximum d'acteurs et l'étude des enjeux et solutions possibles, comme celle entreprise par la Commission, contribue à l'essor des SIA tout en assurant leur utilisation encadrée et responsable.

6. SYNTHÈSE DES RECOMMANDATIONS

La définition de la notion de renseignement personnel

1. Le critère en vertu duquel une donnée doit permettre l'identification pour être considéré comme un renseignement personnel devrait être abandonné ;

2. Les inférences, profils, prédictions et résultat de décisions automatisées devraient être considérés comme des renseignements personnels s'ils concernent une personne physique ;

3. Les renseignements rendus non identifiables devraient être couverts par les lois de protection des renseignements personnels.

4. L'inférence de renseignements personnels à partir d'un algorithme ainsi que les activités de profilage, d'analyse et de prédiction devraient être encadrés par le biais de la notion de traitement de renseignement personnel à haut risque.

Minimisation des données : les principes de limitation et de détermination des fins

5. L'approche minimaliste en matière de traitement des renseignements personnels ne doit pas être abandonnée.

6. Le principe de détermination des fins ne doit pas être abandonné. Malgré le fait qu'il est difficile d'identifier les finalités précises de l'utilisation de renseignements personnels, les entreprises et les organisations qui traitent des données devraient être en mesure de formuler des objectifs généraux.

7. Le critère de nécessité comme moyen d'opérationnaliser l'approche minimaliste devrait être abandonné au profit du critère de légitimité.

8. Certaines fins illégitimes devraient être identifiées pour l'application du critère de légitimité du traitement de renseignements personnels.

L'individu en contrôle : les principes de consentement, d'accès à l'information et d'exactitude

9. L'importance de la capacité d'un individu à exercer un contrôle sur les modalités de circulation et de diffusion de ses renseignements personnels devrait être réaffirmée ;
10. Les traitements de renseignements personnels à haut risque devraient faire l'objet d'un consentement explicite et adopter une logique « opt-in » ou bénéficier d'une autorisation écrite de la Commission pour être autorisés ;
11. Les données rendues non identifiables devraient pouvoir être réutilisées sans nouveau consentement par l'organisation ou l'entreprise les ayant collectées initialement ;

12. Un droit de refuser de faire l'objet d'un traitement de renseignements personnels à haut risque devrait être prévu explicitement ;

13. Un droit de recevoir une explication, garantie par un professionnel, de la logique sur laquelle une prédiction ou une décision automatisée est fondée et dans la mesure du possible, une explication des facteurs et des paramètres les plus importants ayant mené à la prise d'une décision devrait être prévue.

14. Il faut étendre le droit à la suppression des renseignements personnels aux inférences, profils et résultats de décisions automatisées.

15. Les renseignements personnels ayant fait l'objet d'un traitement automatisé qui sont inexacts, incomplets ou équivoques peuvent être révisés par un être humain ou être supprimés.

Principes de responsabilité démontrable et de transparence

16. La commission devrait jouer le rôle de responsable de la transparence institutionnelle en matière de protection des renseignements personnels.

17. Les entreprises et les organisations qui traitent des renseignements personnels devraient avoir l'obligation d'adopter un cadre de gouvernance des données.

18. La Commission devrait adapter l'outil de l'évaluation d'incidence algorithmique du gouvernement canadien à ses réalités et l'adopter pour la conduite des évaluations d'impacts relatifs à la protection des données.

19. Les pénalités pour manquements aux obligations en matière de protection des renseignements personnels devraient être fixées en fonction du chiffre d'affaires annuel mondial.