Commission
de l'éthique
en science
et en technologie
Québec

RÉPONSE AU DOCUMENT DE CONSULTATION SUR L'INTELLIGENCE ARTIFICIELLE DE LA COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC

Mémoire présenté à la
Commission d'accès à l'information du Québec

Dans le cadre du
Document de consultation – Intelligence artificielle

Par la
Commission de l'éthique en science et en technologie

Mai 2020

Commission de l'éthique en science et en technologie
888, rue Saint-Jean, bureau 555
Québec, QC
G1R 5H6

Document préparé par
Nathalie Torrès-Parent, B.A., conseillère en éthique

Direction
Sylvain Pelletier, M.A., secrétaire général

TABLE DES MATIÈRES

Présentation

Ce mémoire est présenté par la Commission de l'éthique en science et en technologie (CEST), un organisme du gouvernement du Québec placé sous la responsabilité du ministre de l'Économie et de l'Innovation. Elle est composée de 13 membres, dont un président, nommés par le gouvernement.

Sa mission est de conseiller le ministre sur toute question relative aux enjeux éthiques liés à la science et à la technologie, ainsi que de susciter la réflexion sur ces enjeux éthiques. De façon générale, ses activités visent à informer, à sensibiliser et à organiser des débats autour des enjeux éthiques en science et en technologie. La CEST propose également des orientations susceptibles de guider les acteurs concernés dans leur prise de décision.

Il se dégage, au sein de l'administration publique, une volonté de mettre davantage à profit les technologies numériques à des fins d'efficience et d'amélioration de la prestation des services publics — ce dont fait foi la Stratégie de transformation numérique 2019-2023. Dans cette foulée, la Commission entend fournir un éclairage sur les enjeux éthiques inhérents aux pratiques gouvernementales touchant le numérique, notamment l'utilisation des données massives et le partage des renseignements personnels entre organismes publics. Elle vise ainsi à aiguiller les acteurs concernés quant aux mesures propres à minimiser les risques et à maximiser les bienfaits de l'usage des données du point de vue de l'intérêt collectif et du respect des droits fondamentaux.

L'analyse éthique des impacts de l'utilisation des données et des systèmes d'intelligence artificielle (SIA) qui en facilite le traitement permet, entre autres, de mettre en relief des enjeux éthiques relatifs à la protection de la vie privée. En ce sens, les travaux de la CEST entrent en résonnance avec les réflexions de la Commission de l'accès à l'information à propos des enjeux de protection des renseignements personnels soulevés par le recours aux SIA.

Sommaire

En réponse au *Document de consultation – Intelligence artificielle* rédigé par la CAI au sujet du renforcement, la CEST présente ce mémoire visant à commenter les principes sous-jacents au renforcement de la protection des renseignements personnels dans un contexte d'exploitation des systèmes d'intelligence artificielle (SIA). Les nouvelles possibilités numériques, dont l'usage des données massives ou d'algorithmes à des fins d'analyse prédictive, poussent à revisiter les cadres normatifs en vigueur. Un consensus réunit les chercheurs quant aux écueils de l'encadrement actuel sur le plan de la protection de la vie privée et quant à la pertinence de les pallier, notamment par un cadre de référence qui met l'accent sur les principes de transparence, de respect de l'autonomie des individus et de responsabilité des organisations à l'égard du traitement des données.

De manière plus précise, les principes présentés par la CAI s'articulent autour de :

- L'encadrement de la création et de l'utilisation de renseignements inférés ;
- L'interdiction d'utiliser des renseignements personnels à des fins malveillantes ;
- L'utilisation des SIA de manière transparente ;
- Le droit à la révision d'une décision prise par un SIA ;
- L'élargissement de la portée du droit à la rectification ;
- L'adaptation de la gouvernance à la réalité numérique ;
- Le renforcement des moyens de contrôle et d'auditabilité ;
- Les particularités de la recherche et du développement en intelligence artificielle.

La CEST partage l'avis qu'en faveur d'un renforcement de la protection de la vie privée, une attention particulière doit être portée à ces diverses dimensions. Le cadre de gouvernance constitue ici une pierre angulaire, dans la mesure où le respect de ce droit passe par un usage responsable des données. Il ne s'agit donc pas seulement de renforcer le contrôle des individus sur leurs renseignements personnels, notamment par un droit de révision ou de rectification, mais d'adapter la gouvernance des données pour assurer en amont que les considérations relatives à la vie privée imprègnent la conception des SIA et que l'utilisation des données s'effectue au regard de fins légitimes, et ce, durant leur cycle complet.

Pour cela, il importe non seulement d'encadrer l'usage de renseignements personnels, mais aussi l'usage de données non directement identificatoires. Dans la mesure où le recoupement et l'agrégation de ce type de données peuvent permettre la réidentification des personnes et porter ainsi atteinte à la vie privée des individus, une place doit être aménagée dans le cadre législatif pour baliser les pratiques d'inférence ou autres types de réutilisation de données.

1. Introduction

Dans le cadre du projet de consultation mené par la Commission de l'accès à l'information, la CEST entend commenter ici les principes et les mesures proposés par la CAI dans l'optique de renforcer la réponse aux enjeux de la protection des renseignements personnels sous-jacents à l'exploitation des systèmes d'intelligence artificielle.

Parmi les principaux enjeux éthiques soulevés par l'intelligence artificielle et le traitement des données massives qu'elle rend possible, la protection des renseignements personnels et plus généralement de la vie privée se pose avec acuité. Au regard du contexte numérique actuel, cerner l'enjeu du respect de la vie privée commande d'élargir la réflexion au-delà de la protection des renseignements personnels[1]. Notamment, le recoupement et l'agrégation des données — qu'elles soient personnelles ou non — comportent des risques d'atteinte à la vie privée des individus, en ce qu'ils peuvent tout de même déboucher vers l'identification des personnes[2] ou vers des pratiques de profilage non identificatoires, mais néanmoins susceptibles de porter préjudice à l'autonomie et à la dignité de membres de la population, des valeurs qui sont intimement liées à la notion de vie privée.

D'ailleurs, ce risque subsiste même s'il y a eu en amont une dépersonnalisation ou anonymisation des données[3], d'où l'intérêt porté aux mesures de sécurité mises en place pour assurer la protection des données et leur confidentialité. Alors qu'il émane des réflexions sur la protection de la vie privée l'importance du contrôle de l'individu sur ses données, fondée sur la valorisation de l'autonomie de l'individu, ainsi que des conditions permettant d'exercer ce contrôle, il devient cependant difficile d'informer les individus sur la gamme d'utilisations potentielles de leurs données et de recueillir ainsi un consentement éclairé[4].

De fait, les données collectées peuvent faire l'objet d'utilisations secondaires par des tiers en vertu de fins autres que celles déterminées initialement. Il s'agit ici d'un enjeu particulièrement saillant en contexte d'exploitation de SIA. C'est pourquoi l'encadrement en matière de données soulève des questionnements sur le cycle complet des données, dont leur diffusion et leur utilisation ultérieure[5,6]. Cela amène aussi à interroger les conditions

[1] Metcalf, J. et al. (The Council for Big Data, Ethics and Society), (2016), « Perspectives on Big Data, Ethics, and Society», *IEEE Access*, vol.2, p. 1-36.
[2] Xavis, V. et al. (2019), « An Ethical Framework for Big Data in Health and Research », *Asian Bioethics Review*, vol. 11, nº 3, p.227-254.
[3] Vayena, E. et al. (2016), « Elements of a New Ethical Framework for Big Data Research», *Washington and Lee Law Review Online*, vol. 72, nº 3, p.420-441.
[4] Xavis, V. et al. (2019), « An Ethical Framework for Big Data in Health and Research », *Asian Bioethics Review*, vol. 11, nº 3, p.227-254.
[5] Vayena, E. et al. (2016), « Elements of a New Ethical Framework for Big Data Research », *Washington and Lee Law Review Online*, vol. 72, nº 3, p.420-441.
[6] Colleman, J. et S.A. Matei (2016), *Ethical Reasoning in Big Data : An Exploratory Analysis*, Collmann, Jeff, 192 p.

dans lesquelles peuvent s'effectuer le transfert et la manipulation des informations[7], de manière à pallier le risque d'utilisations indésirables. D'autant plus que l'utilisation de ces informations peut servir à des fins d'analyses prédictives, lesquelles comportent le risque de renforcer des formes de stigmatisation et de profilage au sein de la population et donner lieu ainsi à un traitement inéquitable. Cela dit, l'enjeu d'encadrement des données tout au long du cycle soulève des difficultés notables, en raison de la mobilité extrême des données.

Dans une telle optique, ce n'est donc pas seulement le caractère personnel des données colligées qui peut s'avérer problématique, mais la finalité de leur usage[8] et la traçabilité de leur cycle complet. Cela signifie de tenir compte du potentiel recoupement et agrégation des données et des risques éthiques de cette possibilité numérique.

Tel qu'il en ressort ici, les capacités de traitement informatique soulèvent des risques sur le plan de la stigmatisation et de la protection du droit à la vie privée. Compte tenu du contexte numérique actuel et plus précisément des enjeux éthiques sous-jacents à l'utilisation des SIA, la CEST est d'avis qu'il est opportun d'opérer des modifications législatives afin de pallier les risques de l'IA sur la vie privée. Les principes proposés à cette fin par la CAI seront ici commentés, à la lumière de la littérature récente et des éléments de réflexion dégagés par la CEST dans ses travaux antérieurs ou en cours (le *trading* haute fréquence, la ville intelligente ou l'encadrement des données massives en contexte d'administration publique). De manière plus précise, il s'agit d'exposer l'accord ou non avec les principes proposés par la CAI et, s'il y a lieu, d'approfondir les enjeux relatifs à la mise en application de ces principes, en pointant notamment des éléments de réflexion supplémentaires sur l'encadrement des SIA.

2. Encadrer la création et l'utilisation de renseignements inférés

2.1 L'inférence ou la création de renseignements personnels à partir d'un algorithme devraient être limitées, en application du critère de nécessité.

Des inférences à partir de données, sans être interdites, exigent tout de même un encadrement pour un usage responsable et éthique. La CEST est d'avis que les inférences et la création de renseignements personnels devraient être limitées, en application du critère de nécessité. Il importerait toutefois de préciser les contours de la notion de nécessité, que ce soit dans le secteur public ou privé. Selon l'article 64 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, il est stipulé que « nul ne peut, au nom d'un organisme public, recueillir un renseignement personnel si cela n'est pas *nécessaire* à l'exercice des attributions de cet organisme ou à la mise en

[7] Green, P. et B. Baumal (2019), « Legal, Ethical and Privacy Issues Affecting Data Sharing Among Ontario's Higher Education Institutions in Interinstitutional Collaboration », *College Quarterly*, vol. 22, nº 2.

[8] Wachter, S. & B. Mittelstadt (2019),« A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI», *Columbus Law Review*, nº2, p.1-131.

œuvre d'un programme dont il a la gestion »[9]. La question subsiste néanmoins à savoir si l'exercice des attributions de l'organisme est acceptable sur le plan éthique.

D'autres principes peuvent aussi être pris en compte pour veiller à ce que le critère de nécessité s'arrime à des projets dont la finalité est légitime. Certains évoqueront à ce propos le principe de justification de l'inférence[10].

En tant qu'elles fournissent des informations sur les individus et qu'elles ont un impact sur leur identité et leur vie, les inférences devraient être soumises à des critères de manipulation pour assurer le respect du droit fondamental de la protection de la vie privée, au même titre que la collecte de renseignements personnels. De fait, bien que certains renseignements collectés au départ puissent ne pas être considérés comme des données sensibles, leur agrégation et les inférences qui en découlent peuvent déboucher sur la création de renseignements personnels et donner lieu à des pratiques de profilage susceptibles de porter préjudice aux individus. Or, à l'heure actuelle, les individus détiennent peu de protection en matière d'inférences ou de renseignements personnels créés à partir d'algorithmes.

Des chercheurs pointent ici l'idée d'introduire dans la sphère législative le droit aux inférences raisonnables (*right to reasonable inferences*) pour protéger les individus d'inférences générées par le traitement de données massives et qui portent atteinte à leur vie privée, leur identité et leur réputation. Dans cette optique, il serait attendu que les responsables de l'utilisation des données soient en mesure de fournir en amont une justification des inférences à effectuer. Plus précisément, les responsables devraient étayer les raisons pour lesquelles les données choisies sont appropriées pour établir des inférences, ainsi que la pertinence des résultats inférés au regard de leur caractère moralement acceptable. Ils devraient aussi employer des méthodes éprouvées sur le plan de la fiabilité[11] et tenir compte des enjeux éthiques de l'accès à des données de qualité et exemptes de biais discriminatoires, de même que des risques de corrélations fallacieuses[12]. Certes, l'efficacité de plusieurs SIA réside souvent dans la capacité de trouver les données appropriées pour mener à bien les inférences, par-delà les capacités cognitives humaines. Cela dit, ce type de recours au SIA ne devrait pas exempter les acteurs de l'exigence de justification des données traitées. Outre le critère de nécessité au regard des fins déterminées, les données utilisées devraient faire l'objet d'une attention au regard de leur caractère moralement acceptable.

Mettre l'accent sur le principe de justification pour délimiter les inférences peut également être appréhendé comme un moyen d'en renforcer la légitimité. Car si une décision basée sur une inférence devrait certes être transparente et pouvoir être contestée, selon qu'elle est

---

[9] Québec, *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, art. 64, [en ligne], page consultée le 13 mars 2020.

[10] . Wachter, S. & B. Mittelstadt (2019),« A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI», *Columbus Law Review*, nº2, p.1-131.

[11] Wachter, S. & B. Mittelstadt (2019),« A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI», *Columbus Law Review*, nº2, p.1-131.

[12] Commissaire à l'information et à la protection de la vie privée de l'Ontario (2017), *Big Data Guidelines*, [en ligne], page consultée le 8 mai 2020.

considérée comme erronée ou biaisée, ce principe n'offre qu'un recours a posteriori. D'ailleurs, des limites sont notées sur ce plan, dans la mesure où il en ressort une asymétrie entre le droit des individus et le pouvoir conféré aux utilisateurs de données. Non seulement les données inférées et le raisonnement qui leur est sous-jacent peuvent être difficilement rectifiés ou évalués, mais même lorsque les individus exercent le droit d'effacement en matière de contrôle des données, ces dernières peuvent avoir déjà été partagées à des tiers et donner lieu à des inférences ultérieures[13].

Or, en matière de gouvernance des données, il importe non seulement de mettre en place des dispositifs pour révoquer les inférences qui « repersonnalisent », mais d'adopter un cadre pour s'assurer en amont que les inférences respectent le principe de protection de la vie privée. Dans le cas des inférences générées par les analyses prédictives de ciblage de comportements, ce type d'usage doit aussi faire l'objet d'un usage responsable. Même si, dans certains cas, les effets sur la vie privée sont moindres, l'usage éthique des SIA doit tenir compte des impacts négatifs en matière de biais et de profilage discriminatoire.

En contexte de réutilisation de données par des tiers, les inférences ou des renseignements personnels créés devraient ainsi être limités, et ce, par un usage conforme à la finalité déterminée initialement[14] et aux principes de minimisation et de nécessité des données collectées, ainsi que de justification des inférences. Sur ce point, les balises posées en éthique de la recherche, où il peut être question d'utilisation secondaire des données, pourraient ici jeter un éclairage et nourrir la réflexion éthique de la réutilisation des données dans un contexte d'exploitation de SIA.

2.2 Les activités de profilage, d'analyse et de prédiction devraient être définies dans la loi. La loi devrait prévoir des conditions et des obligations les encadrant

Compte tenu du fait que les activités de profilage, d'analyse et de prédiction peuvent ouvrir la voie à des traitements discriminatoires à l'égard de certaines franges de population, que les renseignements colligés soient personnels ou non, il est de mise de définir dans la loi sur les secteurs public et privé les conditions et les obligations les encadrant. Il convient cependant de définir en amont ces activités et ce qu'elles couvrent, dans la mesure où il ne se dégage pas les mêmes enjeux éthiques, selon les types d'usage. De fait, les données massives peuvent nourrir des analyses et des prédictions entreprises à des fins d'évaluation de programmes ou de politiques, sans qu'il ne soit question de prendre une décision ou de porter un jugement sur les individus. Les principes suivants devraient aussi être détaillés quant aux objectifs visés par le profilage :

2.2.1 Interdire l'utilisation de certains types de renseignements personnels afin d'effectuer du profilage (ex : renseignements concernant l'origine raciale ou ethnique, les croyances et les opinions politiques, la santé, l'orientation sexuelle et les renseignements financiers ou biométriques), sauf si certaines conditions prévues dans

[13] Wachter, S. & B. Mittelstadt (2019),« A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI», *Columbus Law Review*, nº2, p.1-131.
[14] Delforge, A. (2018), *Comment réconcilier RGPD et Big Data?*, [en ligne], page consultée le 8 mars 2020.

la loi le permettent ;

Plutôt que de miser sur une interdiction de l'usage de certains types de renseignements pour effectuer du profilage, il semble préférable de se pencher sur les objectifs de cette activité, à la lumière de principes éthiques comme le respect de la vie privée et l'intérêt collectif. D'ailleurs, le critère des renseignements personnels est limité pour dresser les contours d'un usage éthique des données, dans la mesure où l'agrégation de données non personnelles peut tout de même porter atteinte à la vie privée des individus en produisant des informations sensibles. En fait, pratiquement n'importe quelle donnée collectée ouvre la voie à cette possibilité.

C'est davantage le contexte d'usage des données à des fins de profilage qui devrait faire l'objet d'une attention, et ce, en veillant au juste équilibre entre les risques soulevés et les bienfaits raisonnables attendus par l'utilisation des données. Les principes de proportionnalité et de responsabilité peuvent ici servir d'éclairage pour assurer cet équilibre et encadrer l'usage des données. De fait, le profilage se décline en divers cas de figure à géométrie variable en matière de conséquences éthiques. Il est possible, notamment, d'utiliser le profilage à des fins de personnalisation de l'offre publicitaire ou d'amélioration de la prestation des services publics, ce qui ne pose pas nécessairement problème d'un point de vue éthique. En santé publique, des renseignements personnels peuvent être recoupés et agrégés pour mieux cerner l'état de santé de certains groupes de population, ce qui peut être justifié. L'interdiction pourrait être ici disproportionnée et c'est en ce sens qu'il importe d'emblée de préciser la notion de profilage et mettre en place un cadre de gouvernance qui favorise les pratiques responsables. Cela, en assurant le droit des individus de réviser ou de rectifier les décisions les concernant.

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

Désactiver par défaut les paramètres de profilage, d'analyse et de prédiction peut être considérée comme une voie propre à favoriser le **consentement explicite** des individus[15]. En effet, le consentement basé sur un *opt-in*, notamment, épouse les critères d'un consentement éclairé, en ce qu'il favorise la prise en compte d'informations pertinentes avant d'effectuer un choix. Il est possible d'élargir la réflexion du consentement éclairé en explorant les autres types qu'il recouvre, tels le consentement continu ou l'approche du métaconsentement, laquelle permet initialement de se positionner sur les utilisations futures des données au moment de consentir à leur partage[16].

Ce qu'il convient de mettre en surbrillance est qu'un consentement doit, pour être valide, réunir plusieurs conditions, en l'occurrence être :

- manifeste, c'est-à-dire donné de manière active plutôt que supposé de

[15] Information Commissioner's Office (s.d.), *Consent*, [en ligne], page consultée le 10 mars 2020.
[16] Groupe de recherche interdisciplinaire en informatique de la santé (s.d.). *Et si les citoyens pouvaient donner accès à leurs données de santé à plusieurs projets de recherche en même temps?*, [en ligne], page consultée le 2 mars 2020.

manière implicite ;
- libre, c'est-à-dire donné sans contrainte ;
- éclairé, c'est-à-dire donné en toute connaissance de cause ;
- donné à des fins spécifiques et pour la durée nécessaire à la réalisation de ces fins ;
- révocable, c'est-à-dire qu'il doit avoir la possibilité d'être retiré à tout moment et que, pendant tout le temps où les données sont conservées ou utilisées, toute information pertinente doit être communiquée aux personnes ayant donné leur consentement.

Afin de favoriser ce type de consentement, une attention devrait être portée à la qualité de l'information dispensée. Lorsque les personnes concernées présentent une perte d'autonomie, des dispositifs devraient être mis en place pour favoriser leur consentement éclairé. Il en va de même pour les franges de populations mineures ou présentant des restrictions cognitives. La distribution de l'application doit être balisée en tenant compte des limites au consentement et prévoir des mécanismes conséquents.

En clair, le consentement en lui-même ne suffit pas si cela ne s'accompagne pas d'une réflexion sur les conditions de possibilité pour l'exercer de manière éclairée. Parmi les écueils sur ce plan, notons la complexité de l'écosystème numérique et la propension humaine à accepter des conditions d'utilisation, sans prendre le temps et déployer l'énergie nécessaire pour bien comprendre les implications du partage de données. Les solutions adoptées pour soutenir un consentement valable doivent ainsi tenir compte des limites du comportement humain, tel que mis en lumière par les recherches en psychologie[17]. Conséquemment, le poids de la responsabilité des personnes devrait être allégé par des pratiques transparentes et une information claire et accessible, tout en maintenant le principe du consentement pour chacune des finalités poursuivies par la collecte des renseignements. La possibilité d'activer les paramètres de profilage, d'analyse ou de prédiction des organisations pourrait aussi être offerte aux individus.

Cela dit, des questionnements émergent quant à l'étendue de cette possibilité. Par exemple, un consentement explicite serait-il requis pour être exposé à des publications de plateformes comme Facebook, lesquelles reposent sur un profilage ? Selon les cas de figure, l'obligation de désactiver par défaut les paramètres de profilage pourrait ne pas soulever les mêmes enjeux et s'avérer plus ou moins pertinente.

Il est possible, notamment, que cette obligation conduise des organisations à désactiver par défaut des algorithmes, pourtant conçus pour répondre à un intérêt collectif, comme ce serait le cas pour la détection de fraude. La réflexion sur le droit à la désactivation pourrait ici être approfondie en tenant compte de ce type d'arbitrage, où se dégage une tension entre les intérêts individuel et collectif.

2.2.3. Obliger les entreprises et les organismes à faire preuve de transparence dans la création ou l'utilisation de renseignements inférés.

[17] Commissariat à la vie privée du Canada (2016), *Consentement et protection de la vie privée*, [en ligne], page consultée le 10 mars 2020.

L'utilisation de renseignements inférés présente un intérêt pour les décideurs publics, puisqu'ils fournissent des données utiles pour aiguiller le processus décisionnel. Les individus devraient toutefois pouvoir obtenir l'information présidant les choix politiques qui les concernent, d'autant que pour l'instant, des lacunes subsistent sur ce plan. Les données personnelles produites par inférences et servant les activités de profilage sont souvent utilisées à l'insu des individus, sans qu'ils consentent à leur partage. Or, « étant donné que la plupart des individus ne sont pas au courant du fait que les opérateurs en ligne ont obtenu par déduction des informations supplémentaires à leur sujet, il est difficile pour ces derniers de s'opposer au traitement de ces données, et il leur est presque impossible de soumettre une demande pour que ces informations soient, le cas échéant, rectifiées »[18]. Tel qu'il se dégage, ce principe s'avère est intimement lié au contrôle des individus sur leurs données et au respect de leurs droits.

En ce sens, les entreprises et les organismes devraient être obligés à faire preuve de transparence dans la création ou l'utilisation de renseignements inférés. De manière générale, la transparence représente un principe éthique essentiel, autour duquel se dégage un consensus, lorsqu'il s'agit d'assurer un encadrement responsable des SIA[19].

Concrètement, l'application de ce principe devrait se traduire par de l'information dispensée aux sujets sur :

– La poursuite d'activités de profilage et les informations personnelles qu'il génère ;
– La logique sous-tendant le modèle prédictif employé ;
– Les conséquences potentielles du profilage mené sur les personnes[20].

Les détenteurs de données devraient de surcroît fournir de l'information aux individus sur les visées de l'utilisation des renseignements inférés, de même que sur la manière dont ils seront traités[21]. En concordance avec ce qui a été soulevé précédemment à propos des inférences limitées en vertu de leur caractère raisonnable, le principe de transparence devrait se traduire par l'exigence de justifier les choix des données sélectionnées à la base des inférences[22].

Si le consentement explicite des individus concernant l'utilisation de leurs données doit être pris en compte, il est confronté à certains écueils, dont les possibilités de réutilisation et de partage de données. C'est le cas pour un consentement spécifique, où il est difficile pour les individus « [d']anticiper ce à quoi ils consentent », que ce soit sur le plan des

[18] Filippi, P. (2016), « Gouvernance algorithmique : Vie privée et autonomie individuelle à l'ère du Big Data », *Open Data & Data Protection*.
[19] Fjeld, J. et al. (2020), *Principled Artificial Intelligence : Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI*, [en ligne], page consultee le 16 mars 2020.
[20] Commissaire à l'information et à la protection de la vie privée de l'Ontario (2017), *Big Data Guidelines*, [en ligne], page consultée le 8 mai 2020.
[21] Information Commissioner's Office (s.d.), *Rights related to automated decision making including profiling*, [en ligne], page consultee le 16 mars 2020.
[22] Wachter, S. & B. Mittelstadt (2019),« A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI», *Columbus Law Review*, nº2, p.1-131.

nouvelles données générées ou de leur utilisation ultérieure[23]. Ainsi, sans nier l'importance du consentement afin de veiller à la légitimité des pratiques de profilage d'analyse ou de prédiction, il convient de tenir compte des limites du consentement spécifique en promouvant d'autres formes de consentement explicite (le *opt-in*, le méta consentement, etc.). Il ne s'agit pas ici de transférer toute la responsabilité aux individus, mais d'assurer en complément un encadrement responsable de la réutilisation de données[24] par le respect de principes connexes au consentement comme le respect de standards et de conditions de transfert ou de manipulation des données[25].

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

Il pourrait être opportun d'élargir la définition pour inclure toute forme de traitement automatisé de données **à caractère personnel et à caractère non personnel.** En matière de profilage, l'accent ne devrait pas seulement porter sur le type de renseignement utilisé, mais les finalités de ce type d'activité. En effet, des données non personnelles peuvent, lorsque recoupées entre elles et agrégées, culminer tout de même vers la création de données sensibles et déboucher vers la réidentification d'individus. En ce sens, l'encadrement du profilage devrait inclure des balises pour l'utilisation de données non personnelles pour évaluer certains aspects personnels relatifs à une personne physique.

3. Interdire l'utilisation de renseignements personnels à des fins malveillantes

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

La CEST est d'avis que le développement d'un SIA ou l'utilisation de renseignements personnels à l'aide d'un SIA à des fins illégitimes ou avec des intentions malveillantes comme celles de tromper, de stigmatiser des personnes ou de leur causer du tort devraient être interdits. Tout de même, les concepts de « fins illégitimes » et « d'intentions

[23] Filippi, P. (2016), « Gouvernance algorithmique : Vie privée et vie individuelle à l'ère des Big Data », *Open Data & Data Protection*.
[24] Mayer-Schonberger, V. (2013), « Notice and consent in a world of Big Data », International Data Privacy Law, vol. 3, nº 2, p. 67-73.
[25] Green, P. et B. Baumal (2019), « Legal, Ethical and Privacy Issues Affecting Data Sharing Among Ontario's Higher Education Institutions in Interinstitutional Collaboration », *College Quarterly*, vol. 22, nº 2.

malveillantes » devraient être définis afin d'assurer une compréhension commune de ce qu'ils désignent. L'atteinte aux droits fondamentaux peut être envisagée ici comme une pierre angulaire dans la formulation de ce qui constitue une fin illégitime. Afin d'assurer une limitation acceptable de l'utilisation des SIA, il est également possible de prendre appui sur d'autres principes.

Compte tenu des risques de l'utilisation des SIA, même lorsque les fins poursuivies sont légitimes, il peut être avisé d'élargir l'encadrement de l'usage de renseignements par-delà les intentions pour tenir compte des conséquences potentielles. Dans cette veine, des réflexions s'imposent quant à la qualité des infrastructures numériques, faute de quoi les droits fondamentaux comme celui de la vie privée ne pourront être respectés. Pour minimiser les risques d'utilisation à des fins malveillantes, il convient ainsi de mettre en place des moyens appropriés, dont des mesures de sécurité robustes[26].

4. Utiliser les SIA de manière transparente

4.1 Les entreprises et les organismes publics devraient obligatoirement divulguer l'utilisation d'un SIA, dès lors qu'une personne entre en interaction directe avec celui-ci, au moment d'une collecte de renseignements personnels ou dans le cadre d'une prestation de services

Comme il ressort de la recension des écrits sur les principes éthiques en matière d'encadrement d'IA, une notification dispensée dès lors qu'une personne entre en interaction directe avec un SIA s'articule au principe éthique du contrôle humain sur la technologie[27], soit une composante récurrente des cadres éthiques en matière d'intelligence artificielle.

Cela dit, dans la pratique, l'actualisation d'une divulgation obligatoire de l'utilisation d'un SIA peut s'avérer problématique. Notamment, en santé publique, où les données colligées, dont des données personnelles, sont agrégées à partir de sources variées, avec la possibilité éventuelle de faire l'objet de traitement par des SIA. Cet exemple soulève des questionnements quant aux modalités de la divulgation obligatoire. Compte tenu de la pluralité des sources de provenance de données, qui assurera cette responsabilité ? La divulgation devrait-elle s'effectuer au moment de la collecte du renseignement personnel ou de manière rétroactive ?

De plus, la divulgation de l'utilisation d'un SIA figure comme une composante parmi d'autres principes sous-tendant la transparence. Une attention devrait ainsi être portée à la justification de l'usage des algorithmes, à leur mécanisme de fonctionnement ou aux dispositifs mis à la disposition des individus pour les contester[28].

---

[26] Commissaire à l'information et à la protection de la vie privée de l'Ontario (2017), *Big Data Guidelines*, [en ligne], page consultée le 8 mai 2020.
[27] Fjeld, J. et al. (2020), *Principled Artificial Intelligence : Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI*, [en ligne], page consultee le 16 mars 2020.
[28] Chignard, S. et S. Penicaud (2019), « With great power comes great responsibility : keeping public sector algorithms accountable », *Medical Journal of Australia*, vol. 200, nº6, p.321.

4.2 Une personne devrait être informée, au moment d'une collecte de renseignements personnels, que d'autres renseignements seront inférés de manière automatique à son sujet, que les données serviront à des activités de profilage, d'analyse ou de prédiction ou qu'une décision sera prise automatiquement à partir des informations qu'elle fournit

La CEST s'accorde avec ce principe, dans la mesure où il fait partie des conditions à mettre en place pour favoriser un consentement éclairé. Toutefois, certains contextes appellent à une modulation de ce principe, dans la mesure où ils ne s'y prêtent pas au même titre que d'autres. En contexte de prestation de soin, par exemple, cette exigence n'est peut-être pas réaliste.

4.3 Une personne doit pouvoir exiger obtenir29 une explication des facteurs et des paramètres les plus importants ayant mené à la prise d'une décision et de la logique du mécanisme de traitement automatisé utilisé pour la prendre, ainsi que de la liste des renseignements personnels utilisés

Utiliser les SIA de manière transparente signifie notamment de souscrire au principe d'explicabilité[30], lequel renvoie à la mise au jour de l'architecture informatique (explicabilité de la procédure) ainsi que des raisons du résultat généré (explicabilité de la décision). D'un point de vue éthique, cette dernière dimension revêt une importance particulière[31], puisqu'il s'agit non seulement de comprendre les paramètres sous-tendant la décision, mais d'interroger la légitimité de cette dernière.

La première modalité d'explicabilité renvoie au fonctionnement des systèmes algorithmiques, en l'occurrence l'explication des facteurs les plus importants ayant mené à la prise d'une décision, la liste des renseignements personnels utilisés ainsi que la logique du mécanisme automatisé sous-jacente. Pour cela, il convient de préciser la nature des concepts sous-jacents à ce droit comme les « paramètres les plus importants ayant mené à la prise de décision » ou la « logique de mécanisme de traitement automatisé ». Ce dernier point devrait non seulement ouvrir la voie à des réflexions sur le fonctionnement général du SIA, mais la manière dont les informations personnelles sont utilisées pour soutenir le processus décisionnel[32]. Certains mentionnent en ce sens la pertinence de baliser de manière claire les éléments devant être fournis par les contrôleurs de données, dont la pondération des caractéristiques, l'arborescence du processus décisionnel ou le système de classification mis en jeu[33].

Cependant, rendre effectif le principe d'explicabilité du fonctionnement en matière de

[29] La formulation pourrait être revisitée pour ne conserver qu'un des deux termes «exiger» ou «obtenir», dans la mesure où ils renvoient à des responsabilités différentes.
[30] Fjeld, J. et al. (2020), *Principled Artificial Intelligence : Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI*, [en ligne], page consultee le 16 mars 2020.
[31] Maclure, J. et M.N. Saint-Pierre (2018), *Le nouvel âge de l'intelligence artificielle : une synthèse des enjeux éthiques*, [en ligne], page consultée le 2 mai 2020.
[32] Edwards, L. et al. (2018), « Enslaving the Algorithm : From a "Right to an Explanation" to a "Right to Better Decisions" ?», *IEEE Security & privacy*, vol. 16, nº 3, p. 46-54.
[33] Wachter, S. et al. (2017), « Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation », *International Data Privacy Law*, vol. 7, nº 2. P. 76-99.

traitement automatisé demeure un enjeu, pour des raisons techniques, en ce que le cheminement des algorithmes des SIA peut être difficilement retraçable et soulever ainsi le défi de l'intelligibilité des résultats obtenus. Au regard de cet écueil, il est fait mention de développer des « procédures, outils et méthodes permettant d'auditer ces systèmes afin d'en évaluer la conformité à notre cadre juridique et éthique. C'est aussi nécessaire en cas de litige entre différentes parties mettant en cause les décisions prises par des systèmes d'IA. À ce jour, ces capacités, même a posteriori, sont quasi inexistantes, et ce pour diverses raisons. En premier lieu, les techniques d'apprentissage profond sont encore trop opaques […] et leur protocole d'audit encore balbutiant »[34].

Cela étant, même si l'on assurait l'intelligibilité de la logique du mécanisme automatisé, l'explicabilité du fonctionnement ne permet pas d'évaluer la légitimité de la décision. Car bien que cette logique soit mise au jour, son caractère éthique reste à interroger, notamment sur le plan des biais discriminatoires qu'il recèle ou des préjudices qu'ils portent à des groupes de population[35]. Ce qui importe ici, c'est surtout l'explicabilité des résultats obtenus par les SIA, en vertu de laquelle les finalités et les justifications présidant l'utilisation des SIA doivent être exposées [36]. Pour cela, il ne suffit pas de révéler avec transparence les caractéristiques techniques du SIA, mais de se pencher sur la portée normative de ce dernier, c'est-à-dire sur son contexte d'usage et ses impacts sociaux[37].

Dans cette veine, Edwards et Veale incluent dans l'analyse les effets de certaines décisions automatisées à l'échelle collective et non seulement individuelle, en ce que certains mécanismes automatiques peuvent être raisonnables, lorsque pris isolément, mais s'avérer problématique dans leur forme agrégée. C'est le cas notamment de la personnalisation des algorithmes en fonction des préférences de chacun qui alimente les « chambres à écho » potentiellement nuisibles sur le plan de la démocratie[38]. Aussi, certains biais algorithmiques discriminatoires ne sont décelables que par la prise en compte de l'ensemble des données colligées et non seulement par la liste de renseignements d'un seul individu.

D'autres chercheurs invitent aussi à prolonger la réflexion sur l'explicabilité en tenant compte des tensions pouvant advenir entre ce principe et celui du respect d'autres droits, comme la protection de la propriété intellectuelle ou du secret des affaires à des fins de préservation de sécurité et d'ordre public[39,40]. C'est pourquoi il peut être indiqué de recourir

---

[34] Villani, C. et al. (2018), *Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne*, [en ligne], page consultée le 4 mai 2020.
[35] Edwards, L. et M. Veale (2018), « Enslaving the algorithm: from a " right to an explanation" to a "right for better decisions*"?»*, *IEEE Security & Privacy*, vol. 16, nº3, p.46-54.
[36] Uni Global Union (s.d.), *Top 10 Principles – For Ethical Artificial Intelligence*, [en ligne], page consultée le 18 mars 2020.
[37] Pégny, M. et I. Ibnouhsein (2018), « Quelle transparence pour les algorithmes d'apprentissage machine ? », *Revue d'intellignece artificielle*, vol. 32, nº 4, p. 447-478.
[38] Edwards, L. et M. Veale (2018), « Enslaving the algorithm: from a " right to an explanation" to a "right for better decisions*"?»*, *IEEE Security & Privacy*, vol. 16, nº3, p.46-54.
[39] Wachter, S. & B. Mittelstadt (2019),« A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI», *Columbus Law Review*, nº2, p.1-131.
[40] Villani, C. et al. (2018), *Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne*, [en ligne], page consultée le 4 mai 2020.

à un organe indépendant pour assurer l'équilibre entre ces principes en friction[41]. Par ailleurs, des recours collectifs pourraient accompagner ce droit afin de ne pas imposer « une charge importante aux individus pour mettre au jour les explications les concernant et relever les défis qui se présentent à eux »[42].

4.4 Le cadre de gouvernance d'une entreprise ou d'une organisation qui utilise un SIA (voir principe 11) devrait être accessible pour qui en fait la demande, ou devrait être diffusé de façon proactive.

Il est suggéré de diffuser le cadre de gouvernance pour les entreprises ou les organisations qui utilisent un SIA. À des fins de transparence, l'information diffusée devrait décrire la nature des projets sous-tendant l'utilisation de données[43].

5. Établir un droit à la révision d'une décision prise par un SIA

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

Il semble opportun d'exiger une révision par une personne physique d'une décision prise initialement par un SIA. Certaines recommandations en matière d'encadrement éthique de l'IA suggèrent même d'étendre ce droit à la contestation de l'usage de l'IA en matière de décision[44,45]. Plus précisément, ce droit pourrait se concrétiser par une enquête sur les raisons de l'erreur et, conséquemment, une mise à jour les données et le SIA, de manière à éviter la reproduction des erreurs identifiées.

Le droit de révision doit toutefois, pour être effectif, s'accompagner d'information claire quant aux procédures pour exercer ce droit[46]. Notons aussi que ce droit de révision recoupe dans plusieurs cas celui d'obtenir une justification intelligible pour une décision prise par un SIA.

La voie pourrait aussi être explorée d'étendre ce droit aux personnes morales, étant donné la porosité de la frontière entre personnes physiques et morales dans certains cas de figure. Par exemple, il est possible d'imaginer des algorithmes de détection de fraude plaçant sur le radar des microentreprises. Quoiqu'il s'agisse ici de personnes morales, le droit de révision pourrait s'appliquer également. Il pourrait en être de même pour le principe

[41] Wachter, S. & B. Mittelstadt (2019),« A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI», *Columbus Law Review*, nº2, p.1-131.
[42] Edwards, L. et M. Veale (2018), « Enslaving the algorithm: from a " right to an explanation" to a "right for better decisions*"?»*, *IEEE Security & Privacy*, vol. 16, nº3, p.46-54.
[43] Commissaire à l'information et à la protection de la vie privée de l'Ontario (2017), *Big Data Guidelines*, [en ligne], page consultée le 8 mai 2020.
[44] Access Now (2018), *Human Rights in the Age of Artificial Intelligence*, [en ligne], page consultee le 9 mars 2020.
[45] The Toronto Declaration (2018), *The Toronto Declaration : Protecting the right to equality and non-discrimination in machine learning systems*, [en ligne], page consultée le 12 mars 2020.
[46] Fjeld, J. et al. (2020), *Principled Artificial Intelligence : Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI*, [en ligne], page consultee le 16 mars 2020.

suivant portant sur le droit à la rectification.

6. Élargir le droit à la rectification

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

Il importe d'assurer un droit de rectification aux situations où la création ou l'inférence de renseignements personnels n'était pas autorisée par la loi. Tout comme pour le droit de révision, la rectification pourrait sous-tendre l'identification des causes de l'erreur et la modification de renseignements pour éviter qu'elle se reproduise. L'enjeu ici serait toutefois de faire reposer l'entièreté de la responsabilité de la rectification des infractions sur les épaules des individus. Des mécanismes de protection connexes devraient ainsi appuyer ce droit. Le cadre de gouvernance devrait aussi prévoir des lignes directrices sur la manipulation de données, en accord avec la loi et les valeurs et principes éthiques entourant l'usage des SIA.

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

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

Le premier principe proposé comporte un risque d'ouvrir à des possibilités d'abus s'il ne s'accompagne d'aucune obligation pour la personne concernée de justifier les raisons pour lesquelles le renseignement inféré devrait être rectifié. Bien qu'il soit difficile de démontrer le caractère inexact en cas de renseignement inféré, il pourrait tout de même y avoir une nécessité de démontrer un préjudice ou de recourir à une révision du renseignement avant d'en exiger une rectification. Le même raisonnement s'applique au deuxième principe proposé voulant qu'un recours plus spécifique à la nature de ce type de renseignement devrait être prévu, soit le droit de modifier l'inférence, l'opinion, le jugement ou la qualification réalisés par un système automatisé.

Au sein du RGPD, le droit de rectification se définit comme suit : « la personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la **rectification des données à caractère personnel la concernant qui sont inexactes**. Compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire »[47]. Pour être effectif, le droit de rectification doit donc prendre appui sur d'autres critères qui permettent de le justifier — en l'occurrence ici, l'exactitude du renseignement.

[47] GDPR. Expert (s.d.), *Article 16- droit de rectification*, [en ligne], page consultée le 7 mai 2020.

7. Adapter la gouvernance à la réalité numérique

7.1 Obliger les entreprises et les organismes publics à adopter un cadre de gouvernance de la protection des renseignements personnels (accountability)

Au regard des enjeux éthiques entourant la manipulation des données, les autorités responsables ne sauraient faire l'économie d'un cadre de gouvernance. En ce sens, il convient d'**obliger les entreprises et les organismes publics à adopter un cadre de gouvernance de la protection des renseignements personnels**.

Si la gouvernance est modulable selon la particularité des contextes, un consensus se dégage quant au caractère multidimensionnel de ce cadre afin de soutenir une utilisation responsable et éthique des données. La CEST est d'avis qu'il importe d'étayer la réflexion sur les politiques, directives, procédures et mesures à mettre en place. Au-delà de la clarification des responsabilités de chaque partie prenante, laquelle conditionne une bonne gouvernance des données[48] et de l'obligation de rendre des comptes, le **cadre de gestion devrait inclure des politiques, des directives et des procédures, des mesures d'évaluation et d'atténuation des risques, des vérifications et audits réguliers, des mesures de sensibilisation et de formation pour les gestionnaires et les employés, des mesures de transparence des pratiques de l'organisation en matière de SIA et la documentation pertinente permettant d'attester du traitement des renseignements personnels par le SIA, de la phase de conception à celle de son déploiement**. La documentation permettant d'attester des mesures mises en place devrait être mise à jour et conservée. Ces documents devraient être compréhensibles et accessibles.

D'autres éléments sont à incorporer au sein du cadre de gouvernance. Dans un contexte de données massives où **le partage des données** pose particulièrement des enjeux éthiques, l'ensemble des étapes du cycle des données compte. Cette exigence se heurte toutefois à l'écueil de l'extrême mobilité des données et c'est pourquoi la traçabilité des données devrait faire partie des composantes du cadre de gouvernance en matière de délimitation des rôles et des responsabilités. Cette dimension est essentielle pour vérifier la conformité de l'usage de données à celui consenti initialement, de même que pour repérer les erreurs algorithmiques.

En ce sens, les modalités de partage **devraient être balisées par des protocoles robustes**. À cet effet, il est possible d'élaborer un cadre référentiel sur l'anonymisation des données, au sein duquel sont délimités les responsabilités légales, les codes éthiques et les modalités du partage des données[49]. La mise en place de fiducies de données (*Data Trust*) figure ici possiblement parmi les bonnes pratiques, ce concept désignant la dévolution de la gestion des données à un organe indépendant. Entre autres, ce dispositif est envisagé comme un

[48] National Center for Education Statistics (2017), *SLDS Best Practices Brief: P-20W+*, [en ligne], page consultée le 2 mars 2020.
[49] Eliot, M. et al. (2016), *The Anonymisation Decision-Making Frameowrk*,[en ligne], page consultée le 12 mars 2020.

moyen de renforcer la protection des données personnelles et donc la vie privée[50].

Dans l'optique de « prévenir les accès non autorisés ou les partages inappropriés »[51], une attention particulière est à accorder à **la sécurité des données**, et ce non seulement par des mesures d'évaluation et d'atténuation, mais par une **gestion sécuritaire**. Une quantité croissante d'organisations s'inspirent de normes internationales pour assurer une gestion sécuritaire des données, lesquelles se déclinent en cinq volets :

- La sécurité des données assurée par le personnel : en assurant que les individus manipulant les données aient une formation et une expérience adéquates. Il est fait mention de la nécessité de réserver **la manipulation des données aux acteurs ayant l'autorité pour le faire**[52]. Des chercheurs soulignent l'importance de l'expertise afin de tirer un sens de l'ensemble de données massives, de même que pour déterminer les **standards de données de qualité**[53]. À l'instar de ce que propose le European Commission's High-Level Expert Group, un **protocole de données** (*data protocols*) peut venir ici soutenir les pratiques de gestion[54]. Au-delà des compétences techniques en la matière, il importe toutefois de noter que la manipulation des données appelle une **formation sur le plan éthique**[55,56]. Les acteurs doivent être sensibilités aux enjeux de la manipulation des données sensibles et les utiliser de manière responsable.

- La sécurité des projets : en précisant les procédures d'approbation et de révision des données ;
- La sécurité de l'environnement : en vérifiant que l'infrastructure, les applications et les interfaces utilisées pour transférer les données sont suffisamment robustes, tout en assurant la confidentialité des renseignements ;
- La sécurité des données : en précisant les types et formats de données pouvant être transférées [57];

Si les mesures d'évaluation des risques relèvent d'une question de sécurité, il est possible d'incorporer à la notion de risque les potentiels effets discriminatoires de l'usage des SIA sur l'ensemble de la population. À titre de voie envisageable, une évaluation des risques discriminatoires (*Equality Impact Assessements (EqIAs)*) peut être conduite, telle

[50] Element AI (2019), *Data Trust : A New Tool for Data Governance*, [en ligne], page consultée le 15 mars 2020.
[51] Kirby, E. et al. (2018), *L'accès et le partage d'information par les chercheurs en génomique*, [en ligne], page consultée le 15 mars 2020.
[52] Ministère de l'Éducation nationale et de la Jeunesse (France) (2018), *Le numérique au service de l'École de la confiance,* [en ligne], page consultée le 10 mars 2020.
[53] Koltay, T. (2016), « Data governance, data literacy and the management of data quality », *International Federation of Library Association and Institutions*, vol. 42, nº4, p.303-312.
[54] Fjeld, J. et al. (2020), *Principled Artificial Intelligence : Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI*, [en ligne], page consultee le 16 mars 2020.
[55] Mandinach, E. et E. Gummer (2016), « Data Literacy for Educators: Making it Count in Teacher Preparation and Practice », *Mid-Western Educational Researcher*, vol. 29, nº 1, p. 84-88.
[56] Open Data Institute (2019), *The 2019 Data Skills Framework*,[en ligne], page consultée le 6 mars 2020.
[57] UK Data Service, *Regulating Access to Data – Five Safes*, [en ligne], page consultée le 6 mars 2020.

qu'implantée au Royaume-Uni, et ce, en amont de l'élaboration des politiques publiques[58].

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

La CEST est d'avis que la production d'une évaluation des facteurs relatifs à la vie privée devrait être obligatoire préalablement à la mise en œuvre de tout SIA impliquant des renseignements personnels. Les éléments présentés devraient d'ailleurs être explicités en détail, que ce soit les données exactes à colliger, les mécanismes de protection mis en place (pseudonymisation, anonymisation, etc.), la description des mécanismes d'obfuscation, le processus de destruction des données, etc. Sans une information précise, on ne peut assurer que l'EFVP respecte réellement le droit à la vie privée. De surcroît, les mécanismes et les protocoles de sécurités devraient être éprouvés sur le plan de la fiabilité et faire l'objet d'une justification au regard des données probantes.

En complément, des processus de certification ou d'évaluation supplémentaire devraient s'ajouter comme volets du EFVP. La mise en place d'un comité d'éthique ou d'un organe de surveillance indépendant (*Monitoring Body*) est aussi soulevée comme une piste d'action prometteuse afin d'assurer l'alignement des SIA aux principes éthiques[59]. Des critères tels que le respect du principe de minimisation de la collecte, la minimisation des risques ou les mesures de sécurité adéquates devraient orienter les pratiques des acteurs responsables[60].

7.3 Le cadre de gestion, les EFVP et autres audits devraient être révisés périodiquement

La CEST s'accorde avec l'idée que le cadre de gestion, les EFVP et autres audits devraient être révisés périodiquement.

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

La CEST s'accorde pour mentionner que les principes de respect de la vie privée dès la conception (*privacy by design*) et par défaut (*privacy by default*) soient appliqués lors du développement de tout SIA impliquant des renseignements personnels.

En parallèle, certains étofferont la réflexion sur les principes éthiques devant présider la

[58]Edwards, L. et M. Veale (2018), « Enslaving the algorithm: from a " right to an explanation" to a "right for better decisions*"?»*, *IEEE Security & Privacy*, vol. 16, nº3, p.46-54.
[59] Fjeld, J. et al. (2020), *Principled Artificial Intelligence : Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI*, [en ligne], page consultee le 16 mars 2020.
[60] Commissaire à l'information et à la protection de la vie privée de l'Ontario (2017), *Big Data Guidelines*, [en ligne], page consultée le 8 mai 2020.

conception des SIA en soulignant l'importance de l'inclusion (*Inclusiveness by Design*)[61]. Afin de favoriser le caractère éthique des SIA, il est suggéré de diversifier le réseau d'acteurs responsables de leur développement[62]. Cela, tant du point de vue du genre et du bagage culturel que des horizons disciplinaires des chercheurs.

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

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

8. Renforcer les moyens de contrôle et d'auditabilité

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

Les autorités de contrôle, dont la CAI, devraient avoir accès au code des algorithmes à des fins de vérification et de contrôle. Dans son avis sur le trading haute fréquence (THF), la CEST recommandait « aux organismes de réglementation de mettre en place un système d'archivage des algorithmes de THF utilisés sur les plateformes de négociation canadiennes »[63]. Ainsi, en cas d'incident ou de suspicion de manipulation de marché, il est possible de vérifier si l'algorithme est en cause. Le caractère a posteriori de la vérification prend appui sur le secret commercial : les algorithmes devraient demeurer sous protection de propriété intellectuelle et inaccessibles sauf en cas où il est nécessaire d'y avoir accès. Un raisonnement similaire peut s'appliquer ici — à moins qu'il s'agisse aussi de procéder en amont à l'évaluation des algorithmes sur la base d'une EFVP. Le cas échéant, il serait justifié de ne pas uniquement archiver les algorithmes, mais de les rendre accessibles à la CAI, moyennant des garanties en matière de confidentialité et de protection du secret commercial.

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

Compte tenu des risques accrus de la manipulation de renseignements personnels sur le plan de la protection de la vie privée, il semble opportun d'imposer des sanctions dissuasives aux entreprises et organismes en cas de manquement à leurs obligations à l'égard des renseignements personnels, incluant dans le cadre du développement ou de

[61] Fjeld, J. et al. (2020), *Principled Artificial Intelligence : Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI*, [en ligne], page consultee le 16 mars 2020.
[62] Fjeld, J. et al. (2020), *Principled Artificial Intelligence : Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI*, [en ligne], page consultee le 16 mars 2020.
[63] Commission de l'éthique en science et en technologie (2016), *Enjeux éthiques liés au trading haute fréquence*, p. 59.

l'exploitation d'un SIA. Cela dit, les organisations devraient en amont adopter des lignes de conduite pour assurer une gestion responsable des données. Autrement dit, les mécanismes de sanction devraient s'accompagner d'autres mesures pour minimiser les risques en amont de tout projet impliquant la manipulation de données personnelles.

9. Particularités de la recherche et du développement en intelligence artificielle

La recherche appliquée en intelligence artificielle et les phases de développement d'un SIA posent des enjeux particuliers à l'égard de la protection des renseignements personnels. À titre d'exemple, plusieurs affirment qu'un algorithme sera d'autant plus fiable et exempt de biais que les renseignements qui auront été utilisés dans sa période d'entrainement sont nombreux, diversifiés, exacts et de qualité. Ce besoin de données entre en conflit avec le principe de limitation de la collecte.

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

Le principe de limitation de la collecte en contexte de l'utilisation d'un SIA devrait se traduire notamment par le respect du principe de minimisation, lequel contraint le responsable des données « de ne pas traiter plus de données que ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Le responsable doit en effet se limiter à traiter des données adéquates, pertinentes et strictement nécessaires »[64]. Ce principe touche à la fois la quantité et la qualité des données soumises au traitement d'un SIA. D'une part, le nombre de données doit être proportionnel aux fins et, d'autre part, il sous-tend un traitement différencié selon la sensibilité des données.

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

Tout en favorisant l'obtention du consentement, certaines circonstances pourraient rendre acceptable l'utilisation de renseignements personnels lorsqu'il est impossible de l'obtenir[65]. D'autant qu'en contexte de données massives, la notion de consentement se heurte au fait qu'il est difficile de prévoir les usages subséquents des données partagées dans un premier temps. Il conviendrait ainsi de considérer cet enjeu en balisant les modalités de partage et les utilisations ultérieures, et ce, dès la conception des SIA afin d'assurer un usage responsable et éthique des données durant leur cycle complet.

Pour renforcer le droit de regard des individus sur leurs renseignements, certains explorent la possibilité de faire appel à un métaconsentement. Dans la même veine, il est possible de

[64] Delforge, A. (2018), *Comment (ré)concilier RGPD et big data ?*

[65] Pour approfondir cette question, il est possible de se référer à l'Énoncé de politique des trois conseils : Éthique de la recherche avec des êtres humains (EPTC2). Les circonstances rendant acceptables l'utilisation de renseignements personnels lorsqu'il est impossible de l'obtenir y sont explorées.

mettre en place un modèle de consentement élargi, par l'entremise duquel l'individu consent à une activité de collecte de données, en précisant le champ d'activité de recherche pouvant réactualiser ses données, ainsi que les mécanismes de suivi pour assurer un usage qui s'y conforme.

La CEST poursuit ses réflexions en ce qui a trait aux circonstances et aux conditions qui rendraient cette situation acceptable sur le plan éthique. C'est notamment le cas lorsque la valorisation des données sert de façon claire et évidente l'intérêt collectif. La Commission s'avère disposée à travailler conjointement avec la CAI sur cette question.

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

Si l'utilisation de données anonymisées est conçue comme une bonne pratique pour alimenter la recherche au sens large, tout en assurant le respect du droit à la vie privée, plusieurs chercheurs notent les limites des techniques de dé-identification des sujets. En ce sens, si l'utilisation de données anonymisées ou de jeux de données synthétiques pour l'entraînement des SIA est à favoriser pour accroître leur fiabilité et réduire les biais, cette utilisation devrait faire l'objet d'un encadrement spécifique[66]. Outre le respect du principe de pertinence et de proportionnalité de l'usage de données aux finalités du traitement, il est entre autres recommandé de n'utiliser les renseignements personnels que pour la durée du projet[67].

9.4 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 ?

Interdire toute réidentification de données dépersonnalisées est souhaitable sauf en cas de nécessité autorisée ou apparente. Avant de mettre de l'avant ce principe, il pourrait être pertinent de dresser un portrait des différents cas de figure possibles où la réidentification peut être légitime, sans porter atteinte aux droits fondamentaux.

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

La CEST réfléchit actuellement sur ces questions. Elle est disposée à travailler conjointement avec la CAI sur ces questions.

[66] Ohm, P. (2009), « Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization », *UCLA Law Review*, vol. 57, p. 9-12.
[67] Commissaire à l'information et à la protection de la vie privée de l'Ontario (2017), *Big Data Guidelines*, [en ligne], page consultée le 8 mai 2020.